НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___”_____201_ р.

Дипломна робота

на здобуття ступеня бакалавра

з напряму підготовки 6.040301 «Прикладна математика»
(код і назва)

на тему: Застосування квантових алгоритмів Саймона та Бернштейна-Вазірані для криптоаналізу узагальненої мережі Фейстеля

Виконав: студент 4 курсу, групи ФІ-52
(шифр групи)

Шевченко Олексій Тарасович _____
(прізвище, ім’я, по батькові) (підпис)

Керівник к.ф.-м.н. ст. викладач Фесенко Андрій В'ячеславович _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент_____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2019 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут

Кафедра математичних методів захисту інформації

Рівень вищої освіти – перший (бакалаврський)

Напрям підготовки - 6.040301 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою

М.М.Савчук

_____
(підпис) (ініціали, прізвище)

«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту

Шевченку Олексію Тарасовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Застосування квантових алгоритмів Саймона та Бернштейна-Вазірані для криптоаналізу узагальненої мережі Фейстеля, керівник роботи к.ф.-м.н. ст. викладач Фесенко Андрій В'ячеславович,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від _____ р. № _____

2. Термін подання студентом роботи _____

3. Вихідні дані до роботи _____
_____
_____
_____

4. Зміст роботи Побудова атак на узагальнені мережі Фейстеля за допомогою квантових алгоритмів Саймона та Бернштейна-Вазірані, аналіз складності алгоритму Саймона, узагальнення задачі Саймона та застосування цих узагальнень в криптоаналізі криптопримітиву DES-X.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо) _____
_____

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення напряму дослідження	01.09.2018-01.10.2018	
2.	Опрацювання матеріалів по обраній напряму	01.10.2018-01.02.2019	
3.	Узгодження теми дослідження	01.02.2019-01.03.2019	
4.	Аналіз складності алгоритму Саймона	01.03.2019-28.03.2019	
5.	Узагальнення формулювання задачі Саймона	28.03.2019-08.04.2019	
6.	Побудова атак з допомогою отриманих узагальнень	08.04.2019-19.04.2019	
7.	Побудова атак на узагальнену мережу Фейстеля типу 1	19.04.2019-11.05.2019	
8.	Побудова атак на узагальнені мережі Фейстеля типу 2 та 3	11.05.2019-18.05.2019	
9.	Побудова атаки на незбалансовану мережу Фейстеля	18.05.2019-24.05.2019	
10.	Формулювання результатів дослідження	24.05.2019-26.05.2019	
11.	Оформлення роботи	26.05.2019-05.06.2019	

Студент _____ Шевченко О. Т.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Фесенко А. В.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Кваліфікаційна робота містить: 60 сторінок, 11 рисунків та 17 джерел.

В роботі досліджено стійкість узагальнених мереж Фейстеля до квантового диференціального криптоаналізу за допомогою алгоритмів Саймона та Бернштейна-Вазірані. Проведено аналіз алгоритму Саймона та отримано кількісні оцінки складності. Запропоновано узагальнення задачі Саймона та використано його для атаки на криптопримітив DES-X.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту інформації.

Предметом дослідження є стійкість узагальнених мереж Фейстеля до методів диференціального квантового криптоаналізу.

Задачею роботи є побудова атак на узагальнені мережі Фейстеля за допомогою алгоритмів Саймона та Бернштейна-Вазірані, отримання оцінок складності цих атак.

Методами дослідження є методи лінійної алгебри, теорії складності та теорії ймовірності.

Завдання роботи: побудувати квантові атаки розпізнавання на узагальнені мережі Фейстеля, дослідити можливість узагальнення або розширення формулювання задачі Саймона з подальшим використанням, отримати кількісні оцінки складності алгоритму Саймона.

Результати цієї роботи частково представлені на XVII Науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (26-27 квітня 2019 р., м. Київ).

УЗАГАЛЬНЕНА МЕРЕЖА ФЕЙСТЕЛЯ, КВАНТОВИЙ ДИФЕРЕНЦІАЛЬНИЙ КРИПТОАНАЛІЗ, АЛГОРИТМ САЙМОНА, АЛГОРИМТ БЕРНШТЕЙНА-ВАЗІРАНІ

РЕФЕРАТ

Квалификационная работа содержит 60 страниц, 11 рисунков и 17 источников.

В работе исследована стойкость обобщенных сетей Фейстеля к квантовому дифференциальному криптоанализу на основе алгоритмов Саймона и Бернштейна-Вазирани. Проведен анализ алгоритма Саймона и получены количественные оценки сложности. Предложено обобщение задачи Саймона, которое использовано для атаки на криптопримитив DES-X.

Объектом исследования являются информационные процессы в системах криптографической защиты информации.

Предметом исследования является стойкость обобщенных сетей Фейстеля к методам дифференциального квантового криптоанализа.

Задачей работы является построение атак на обобщенные сети Фейстеля с использованием алгоритмов Саймона и Бернштейна-Вазирани, получения оценок сложности этих атак.

Методами исследования являются методы линейной алгебры, теории сложности и теории вероятности.

Задания работы: построить атаки распознавания на обобщенные сети Фейстеля, исследовать возможность обобщения формулировки задачи Саймона с последующим использованием, получить количественные оценки сложности алгоритма Саймона.

Результаты этой работы частично представлены на XVII Научно-практической конференции студентов, аспирантов и молодых ученых « Теоретические и прикладные проблемы физики, математики и информатики » (26-27 апреля 2019, г. Киев).

ОБОБЩЕННАЯ СЕТЬ ФЕЙСТЕЛЯ, КВАНТОВЫЙ ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ, АЛГОРИТМ САЙМОНА, АЛГОРИМТ БЕРНШТЕЙНА-ВАЗИРАНИ

ABSTRACT

The thesis contains: 60 pages, 11 figures and 17 sources.

The resistance of the generalized Feistel networks to quantum differential cryptanalysis using Simon and Bernstein-Vazirani algorithms was investigated in the paper. Simon algorithm complexity was analyzed and obtained estimates of the algorithm complexity. Generalized Simon's problem and proposed usage of it for attacking an cryptographic system DES-X.

The object of the study is information processes in cryptographic security systems.

The subject of the study is the resistance of the generalized Feistel networks to the methods of differential quantum cryptanalysis.

The task of the work is to build attacks on generalized Feistel networks using Simon and Bernstein-Vazirani algorithms, obtain estimates of the complexity of these attacks.

Methods of research are methods of linear algebra, theory of complexity and probability theory.

Tasks of the work: construct quantum recognition attacks on the generalized Feistel networks, explore the possibility of generalizing the Simon's problem with subsequent usage of it, obtain estimates of the complexity of the Simon's algorithm.

The results of this work are partially presented at the XVII Scientific and Practical Conference of Students, Aspirants and Young Scientists "Theoretical and Applied Problems of Physics, Mathematics and Informatics"(April 26-27, 2019, Kyiv).

GENERALIZED FEISTEL NETWORK, QUANTUM DIFFERENTIAL CRYPTANALYSIS, SIMON ALGORITHM, BERNSTEIN-WAZIRAN ALGORITHM

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

$\oplus$ – операція побітового додавання за модулем 2

$\cdot$ – операція скалярного добутку векторів

$O(\cdot)$ – нотація Ландау

$|v\rangle$, $\langle v|$ – нотація Дірака

$\langle \cdot, \cdot \rangle$ – скалярий добуток векторів стану квантової системи

H – перетворення Уолша-Адамара

$nonce$ – криптографічний нонс

$rang(\cdot)$ – ранг системи векторів

$span(\cdot)$ – лінійна оболонка, побудована над системою векторів

$Geom(p)$ – геометричний імовірнісний розподіл з імовірністю успіху p

$E[\cdot]$ – математичне очікавання випадкової величини

$Var[\cdot]$ – дисперсія випадкової величини

$\|$ – операція конкатенації векторів

$Im[f](A)$ – образ множини A відповідно до функції f

$\mathfrak{B}_{n,m}$ – множина всіх функцій, які відображать простір бітових векторів довжини n в простір бітових векторів довжини m.

$S_f(\omega)$ – коефіцієнт Уолша-Адамара функції f в точці ω.

ВСТУП

Актуальність дослідження. З появою перших ідей щодо використання квантової моделі обчислень з'явилась можливість використання цієї моделі обчислень для криптоаналізу різних примітивів. Як виявилось, більшість сучасних асиметричних криптосистем є не стійкими у квантовій моделі обчислень. Причиною цього стало те, що стійкість більшості сучасних асиметричних криптосистем базується на задачах дискретного логарифмування та факторизації цілих чисел, які в класичній моделі мають щонайкраще субекспоненційні алгоритми розв'язку, а при постановці задачі дискретного логарифмування в групі точок еліптичної кривої не знайдено алгоритмів, які мають менше ніж експоненційну складність. Проте в квантовій моделі обчислень ці задачі мають поліноміальний алгоритм розв'язку, що робить неможливим використання цих задач для побудови стійких асиметричних криптосистем.

Однак питання стійкості симетричних криптосистем у загальному випадку залишається відкритим. Існуючий квантовий алгоритм Гровера дозволяє скоротити атаки повного перебору вдвічі відносно розміру задачі.

Одним із новітніх методів криптоаналізу симетричних криптосистем у квантовій моделі обчислень є використання квантових алгоритмів Саймона та Бернштейна-Вазірані. Першою роботою в цьому напрямі була робота Кувакадо та Мораї [1], в якій доведено, що трираундова мережа Фейстеля не є стійкою псевдовипадковою підстановкою в квантовій моделі обчислень. Пізніше на основі цієї роботи в роботах [2], [3] та [4] було представлено атаку на схему Івена-Мансура та атаку підробки повідомлень коду аутентифікації GMAC, покращено атаку раундового зсуву. Ці ідеї розвинуті в роботах [5], [6], [7] та інших. На основі цих алгоритмів в роботі [8] було представлено ідеї квантового диференціального та лінійного криптоаналізу.

Об'єктом дослідження цієї роботи є інформаційні процеси в системах криптографічного захисту інформації

Предмет дослідження – стійкість узагальнених мереж Фейстеля до квантового диференціального криптоаналізу.

Метою роботи є дослідження стійкості узагальнених мереж Фейстеля до квантового диференціального криптоаналізу з використанням алгоритмів Саймона та Бернштейна-Вазірані.

Задачею цієї роботи є побудова атак на узагальнені мережі Фейстеля методами диференціального криптоаналізу на основі квантових алгоритмів Саймона та Бернштейна-Вазірані, отримання оцінок складності цих атак.

Для досягнення мети дослідження, поставлено наступні *завдання*:

1) побудувати атаки на узагальнені мережі Фейстеля типу 1, 2, 3 та незбалансовану мережу Фейстеля за допомогою квантових алгоритмів Саймона та Бернштейна-Вазірані

2) дослідити можливість узагальнення формулювання задачі Саймона для більшого класу функцій, та його застосування в криптоаналізі узагальнених мереж Фейстеля та подібних криптопримітивів

3) отримати кількісні оцінки для часової та просторової складності алгоритму Саймона, для використання в аналізі побудованих атак

При виконанні поставлених задач використовувались такі *методи дослідження*: методи квантового диференціального криптоаналізу, теорія складності, базовий апарат теорії ймовірності та лінійної алгебри.

Практичне значення цієї роботи полягає в отриманні нових методів криптоаналізу симетричних криптопримітивів для побудови стійких криптопримітивів за умови існування квантового комп'ютера. Результати роботи можуть бути застосовані до аналізу існуючих блокових шифрів в квантовій моделі обчислень та побудови шифрів малоресурсної криптографії, що базуються на схемах подібних до мережі Фейстеля, які будуть стійкими до квантових атак на основі обраного відкритого тексту.

Апробація результатів та публікації. Результати цієї роботи частково представлені на XVII Науково-практичній конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики» (26-27 квітня 2019 р., м. Київ).

1 ТЕОРЕТИЧНІ ВІДОМОСТІ З КВАНТОВОГО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ

В цьому розділі наведено необхідні теоретичні відомості достатні для подальшого розуміння роботи. Детально розглянуто квантові алгоритми Саймона та Бернштейна-Вазірані, оскільки всі побудовані атаки будуть базуватися на використанні цих алгоритмів. Сформульовано задачі, які вони розв'язують та показано коректність цих алгоритмів, наведено деякі оцінки їх складності. Представлені найбільш відомі атаки побудовані за допомогою цих алгоритмів, серед яких атака на трираундову мережу Фейстеля та атака підробки повідомлень на GMAC.

1.1 Необхідні теоретичні відомості з теорії квантових обчислень

Для подальшого розуміння роботи наведемо необхідні теоретичні відомості, більшість з яких буде стосуватись теорії квантових обчислень. Детально цей матеріал можна розглянути в книгах [9] та [10], на яких базується цей підрозділ.

Для аналізу складності використовуватимемо нотацію O-велике, яка описує швидкість зростання функції на асимптотиці, відому як нотація Ландау. Ця нотація використовується для оцінки зверху швидкості росту функції.

Означення 1.1. Нотація O-велике

Нехай задано дві функції натурального аргументу $f(n)$ та $g(n)$. Тоді функція f є O-велике від функції g (позначають $f = O(g)$) при $n \longrightarrow +\infty$, якщо існують константи $c > 0$ та $N_0 > 0$ такі, що для будь якого $n > N_0$ виконується нерівність $|f(n)| < |c \cdot g(n)|$.

Розглянемо основи теорії квантових обчислень. Будь-який квантовий алгоритм, фактично, є деякою квантово-механічною системою та набором перетворень над нею. Найпростішою такою системою є **кубіт** – одиниця інформації в квантовій моделі обчислень. Фізична реалізація цієї системи описується хвильовою функцією в двовимірному гільбертовому просторі. Стан такої системи описують за допомогою бра та кет позначень Дірака. Хвильова функція ймовірностей матиме наступний вигляд $\psi = \alpha |0\rangle + \beta |1\rangle$, де для комплексних коефіцієнтів a та b виконується наступне співвідношення $|a|^2 + |b|^2 = 1$. Введемо формальне означення кубіту.

Означення 1.2. Кубітом називається лінійна комбінація станів квантової системи $\psi = \alpha |0\rangle + \beta |1\rangle$, де α, β – комплексні коефіцієнти для яких виконується умова нормування $|a|^2 + |b|^2 = 1$, $|0\rangle, |1\rangle$ – обчислювальний базис.

Операція вимірювання кубіту, фактично, є проекцією на деякі ортогональні простори, після якої відбувається колапс хвильової функції, в наслідок чого система переходить в стан $|0\rangle$ з ймовірністю $|\alpha|^2$, або в стан $|1\rangle$ з ймовірністю $|\beta|^2$.

Узагальнимо поняття кубіта на випадок складної системи.

Означення 1.3. Квантовим регістром довжини n називається квантова система, хвильова функція якої може бути представлена як унітарний вектор в 2^n-вимірному гільбертовому просторі над полем комплексних чисел. Тобто маємо хвильову функцію $\psi = \sum_{i=0}^{2^n-1} \lambda_i |i\rangle$, для коефіцієнтів якої виконується умова нормування $\sum_{i=0}^{2^n-1} |\lambda_i|^2 = 1$.

Розглянемо загальну схему квантових обчислень. Спочатку систему з деякою кількість працюючих сумісно кубітів ініціалізують певним станом. Потім до системи або її підсистеми починають застосовувати певні фізичні перетворення, які математично описуються, як деякі унітарні перетворення в гільбертовому просторі. Впродовж цього процесу квантова система «паралельно» виконує операції над усіма базисними станами, кількість яких зростає з експоненційною швидкістю, як функція довжини квантового

регістру. Після всіх операцій виконують операцію вимірювання над системою або її підсистемою, що і є розв'язком задачі з певною ймовірністю. Для підтвердження правильності розв'язку задачі цю процедуру, зазвичай, виконують декілька разів.

Незважаючи на всі переваги таких систем, у порівнянні з класичними обчислювальними системами, побудова квантової обчислювальної системи стикається з набагато складнішими проблемами реалізація серед яких: декогеренція системи в наслідок взаємодії з зовнішнім середовищем, проблемою фізичної масштабованості системи та проблемами пов'язаними з накопиченням помилки під час обчислень. Слід також зазначити, що побудова квантових алгоритмів є також достатньо складною задачею, оскільки більшість методик побудови алгоритмів в класичній моделі обчислень не застосовні в квантової моделі обчислень.

Математична теорія квантових обчислень повністю базується на наборі постулатів, які й визначають її обчислювальні можливості. Розглянемо ці постулати.

Постулат перший. Простір станів системи асоційований з ізольованою квантово-механічною системою.

Постулат другий. Стан системи в будь-який момент часу повністю описується унітарним вектором у векторному лінійному просторі над полем комплексних чисел з визначеною операцією скалярного добутку.

Постулат третій. Еволюція стану замкненої квантової системи описується тільки унітарними перетвореннями.

Постулат четвертий. Вимірювання стану квантової системи складається з лінійних операторів, що є проекторами на ортогональні підпростори.

Постулат п'ятий. Простір станів складної квантової системи є тензорним добутком просторів станів її складових частин.

І на останок для аналізу алгоритму Саймона застосовується деякий базовий апарат лінійної алгебри, серед якого слід тільки згадати означення лінійної оболонки над системою векторів.

Означення 1.4. Лінійна оболонка над системою векторів

Лінійною оболонкою над системою векторів бітових $\{u_i\}_{i=0}^{n-1}$ називається множина $span(u_0, \ldots, u_{n-1}) = \{x : x = \sum_{i=0}^{n-1} \lambda_i u_i \quad \lambda_i \in F_2\}$.

1.2 Постановка задача Саймона та її розв'язок у квантовій моделі обчислень

Постановка задачі, а також ефективний квантовий алгоритм її розв'язку було представлено в 1994 році в роботі Саймона[11]. Це перший квантовий алгоритм (рис. 1.1), якому достатньо експоненційно меншої кількості запитів до оракула в порівнянні з будь-яким класичним алгоритмом розв'язку.

Задача 1.1. Задача Саймона [11]

Нехай задано функцію $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ за допомогою оракула таку, що для довільних значень $x, y \in \{0,1\}^n$ виконується рівність $f(x) = f(y)$ тоді і тільки тоді, коли $(x \oplus y) \in \{0, s\}$, для деякого невідомого фіксованого значення $s \in \{0,1\}^n$. Необхідно визначити чи існує ненульове значення s та знайти його.

В класичній моделі така задача розв'язується за щонайменше $\Omega(2^{n/2})$ запитів до оракула, навіть з використанням ймовірнісних алгоритмів, а у квантовій моделі обчислень задачу Саймона можна розв'язати, використовуючи $\mathcal{O}(n)$ запитів до оракула.[11]

Розглянемо алгоритм розв'язку, який наведено в роботі [11], і на який посилаються як на квантовий алгоритм Саймона.

Алгоритм 1.1. Квантовий алгоритм Саймона

1) Підготувати два регістри розміру n у стані $|0\rangle\,|0\rangle$.

2) Застосувати перетворення Уолша-Адамара до першого регістру.

3) Використати стандартну модель оракулу, який обчислює значення функції f.

4) Зробити вимірювання другого регістру.

5) Застосувати перетворення Уолша-Адамара до першого регістру.

6) Зробити вимірювання першого регістру. Результатом вимірювання буде деяке випадкове значення $u \in \{0,1\}^n$.

7) Сформувати систему лінійних рівнянь $u_i \cdot s = 0$ рангу $n-1$.

8) Розв'язати систему рівнянь та повернути розв'язок системи.

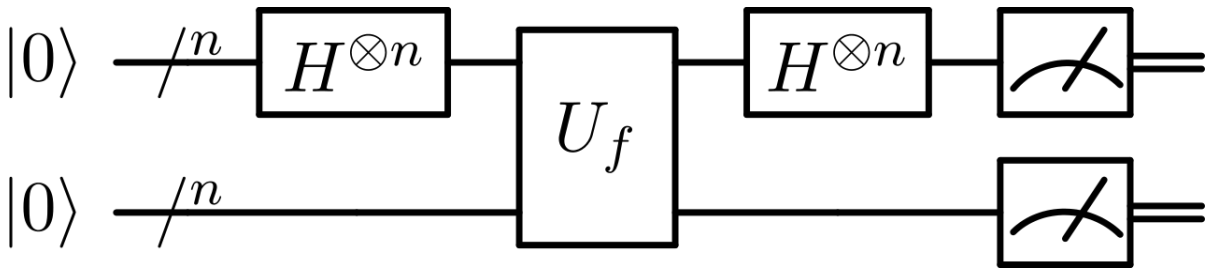

Рисунок 1.1 – Схема квантового алгоритму Саймона

Розглянемо роботу алгоритму в деталях. Після кроку ініціалізації отримуємо систему в стані $\psi_1 = |0\rangle|0\rangle$. Застосовуємо перетворення Уолша-Адамара для стану ψ_1, в результаті отримуємо систему в стані $\psi_2 = (H^{\otimes n} \otimes I_n)\psi_1 = (H^{\otimes n} \otimes I_n)|0\rangle|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in Z_2^n} |x\rangle|0\rangle$. Застосовуємо стандартну модель оракула, яка обчислює значення функції f та отримуємо систему в стан $\psi_3 = U_f(\psi_2) = U_f(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle|0\rangle) = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle|f(x)\rangle$. Після вимірювання другого регістру, перший регістр перейде у стан $\psi_4 = \frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)$ для деякого значення z, де $f(z)$ є результатом вимірювання. Застосовуємо перетворення Адамара до першого регістру $\psi_5 = H^{\otimes n}\psi_4 = H^{\otimes n}(\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)) = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}} \sum_y (-1)^{zy}(1 + (-1)^{sy})|y\rangle$. Зробивши вимірювання першого регістру. Результатом вимірювання буде деяке випадкове значення $u \in \{0,1\}^n$ таке, що $u \cdot s = 0$. Після cn ітерацій цієї процедури отримаємо $n-1$ лінійно незалежних векторів, які є ортогональними до вектора s, де $c > 1$ – деяка константа. В результаті отримуємо систему лінійних рівнянь, розв'язавши яку, обчислюємо значення s та перевіряємо чи є воно тривіальним.

Постановка задачі Саймона вимагає відсутності додаткових колізій

$t \notin \{0, s\}$ таких, що $f(x) = f(x \oplus t)$ для деяких значень x. Проте в роботі [3] доведено, що квантовий алгоритм Саймона розв'язує задачу Саймона навіть при наявності додаткових колізій. На задачу Саймона з можливістю додаткових колізій функції будемо посилатися, як на **узагальнену задачу Саймона**.

Нехай $\epsilon(f, s) = \max_{t \in \{0,1\}^n \setminus \{0,s\}} Pr_x[f(x) = f(x \oplus t)]$ – метрика, яка, пояснюючи неформально, показує, наскільки функція відрізняється від умов оригінальної задачі Саймона. В роботі [3] навели оцінку ймовірності невдачі алгоритму доведення, якої опирається на наступну лему.

Лема 1.1. *Нехай* $t \in \{0,1\}^n$. *Визначимо функцію* $g_t(x) = 2^{-n} \sum_{y \cdot t = 0} (-1)^{x \cdot y}$ *для фіксованого* t. *Тоді* $g_t(x) = \frac{1}{2}(\delta_{x,0} + \delta_{x,t})$

Доведення даної леми наведено в роботі [3], проте воно є достатньо складним, через що, не представлене в цьому розділі. Маючи цю лему можна переходити до доведення теореми про оцінку зверху для ймовірності помилки алгоритму для випадку функції з додатковими колізіями.

Теорема 1.1. *[3]*

Якщо $\epsilon(f, s) = p < 1$, *тоді алгоритм Саймона обчислює значення* s, *використовуючи* cn *запитів до стандартної моделі оракула, який обчислює значення функції, з ймовірністю не менше ніж* $1 - (2(\frac{1+p}{2})^c)^n$

Доведення.

$$
\begin{aligned}
p_{fail} &\leq Pr[rang(span(u_1, \ldots, u_{cn})) < n - 1] \leq \\
&\leq Pr[\exists t \notin \{0, s\} \quad \forall i \quad u_i \cdot t = 0] \leq \\
&\leq \textstyle\sum_t Pr[\forall i \quad u_i \cdot t = 0] \leq \\
&\leq \textstyle\sum_t \prod_i Pr[u_i \cdot t = 0] \leq \\
&\leq \textstyle\sum_t Pr[u_1 \cdot t = 0]^{cn} \leq \\
&\leq 2^n \max_t Pr[u_1 \cdot t = 0]^{cn} = \\
&= \max_t (2Pr[u_1 \cdot t = 0]^c)^n
\end{aligned}
$$

Знайдемо ймовірність $Pr[u_1 \cdot t = 0]$

$$Pr[u_1 \cdot t = 0] = \| 2^{-n} \textstyle\sum_x \sum_{y \cdot t = 0} (-1)^{x \cdot y} |y\rangle |f(x)\rangle \|^2 =$$

$$= 2^{-n} \sum_{y' \cdot t=0} \sum_{y'' \cdot t=0} \langle y'|y''\rangle \sum'_x \sum''_x (-1)^{x' \cdot y'} \langle f(x')| (-1)^{x'' \cdot y''} |f(x'')\rangle =$$
$$= 2^{-n} \sum_{y \cdot t} \sum'_x \sum''_x (-1)^{y \cdot (x' \oplus x'')} \langle f(x')|f(x'')\rangle =$$
$$= 2^{-n} \sum_{x',x''} \langle f(x')|f(x'')\rangle \sum_{y \cdot t=0} (-1)^{y \cdot (x' \oplus x'')} =$$
$$= 2^{-n} \sum_{x',x''} \langle f(x')|f(x'')\rangle \, 2^{n-1} (\delta_{x' \oplus x'',0} + \delta_{x' \oplus x'',t}) =$$
$$= 2^{-(n+1)} (\sum_x \langle f(x)|f(x)\rangle + \sum_x \langle f(x)|f(x \oplus t)\rangle =$$
$$= \tfrac{1}{2}(1 + Pr_x[f(x) = f(x \oplus t)])$$

Отже, маємо $p_{fail} = \max_t (2Pr[u_1 \cdot t = 0]^c)^n = (2(\frac{1+p}{2})^c)^n$ □

Завдяки такому узагальненню, алгоритм Саймона можна застосовувати до класу функцій, які майже задовольняють вимогам оригінальної задачі відповідно до метрики $\epsilon(f, s)$. Як наслідок, якщо $\epsilon(f, s) < \frac{1}{2}$, то ймовірність помилки алгоритму можна зробити як завгодно малою, інакше існує диференціал функції f з ймовірністю більшою за $\frac{1}{2}$ (в цьому випадку застосовними є класичні методи диференціального криптоаналізу).[3]

1.3 Постановка задачі пошуку лінійної структури та її розв'язок в квантовій моделі обчислень

Задача пошуку лінійної структури є узагальненням задачі Саймона, на випадок, коли при зміщені аргументу функції на деякий фіксований вектор, її значення також зміщується на деякий фіксований вектор, для всіх аргументів. Введемо формальне поняття лінійної структури.

Означення 1.5. Лінійна структура булевої функції

Нехай $F \in \mathfrak{B}_{n,m}$ – деяка функція. Вектор $a \in \{0,1\}^n$ називається лінійною структурою функції F, якщо $\forall x \in \{0,1\}^n \quad \exists \alpha \in \{0,1\}^m$ таке, що $F(x) \oplus F(x \oplus a) = \alpha$.

Позначимо через U_F множину всіх лінійних конструкцій функції f. Очевидно, що цю множину можливо представити як $U_F = \bigcup_{\alpha \in \{0,1\}^m} U_f^\alpha$,

де множина $U_F^\alpha = \{a \in \{0,1\}^n : \forall x \in \{0,1\}^n \quad F(x) \oplus F(x \oplus a) = \alpha\}$. Визначимо задачу пошуку лінійної структури для одновимірної функції.

Задача 1.2. Задача пошуку лінійної структури

Нехай задана функція $f : \{0,1\}^n \longrightarrow \{0,1\}$ за допомогою оракула, що має лінійну структуру $a \in \{0,1\}^n$. Необхідно знайти невідоме значення вектора a.

Вперше квантовий алгоритм розв'язку цієї задачі для випадку коли $f(x) = a \cdot x$ було опубліковано в 1997 році в роботі Бернштейна та Вазірані [12]. Цей алгоритм потребував експоненційно меншої кількості запитів до оракула, ніж будь-який класичний алгоритм розв'язку цієї задачі. Наведемо алгоритм, який був представлений в їх роботі.

Алгоритм 1.2. Квантовий алгоритм Бернштейна-Вазірані

1) Підготувати два регістри у стані $|0\rangle^{\otimes n} |1\rangle$.

2) Застосувати перетворення Уолша-Адамара до регістрів.

3) Використати стандартну модель оракулу, який обчислює значення функції f.

4) Застосувати перетворення Уолша-Адамара до першого регістру та відкинути $n+1$ кубіт.

5) Зробити вимірювання першого регістру та повернути це значення.

Розглянемо, як змінюється стан квантової системи впродовж роботи алгоритму. Після ініціалізації квантова система перебуває в стані $\psi_1 = |0\rangle^{\otimes n} |1\rangle$. Застосувавши перетворення Уолша-Адамара до регістрів отримаємо систему $\psi_2 = H^{\otimes(n+1)}\psi_1 = H^{\otimes(n+1)} |0\rangle^{\otimes n} |1\rangle = \sum_{x \in Z_2^n} \frac{|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Використавши стандартну модель оракулу, яка обчислює значення функції f, отримаємо $\psi_3 = U_f(\psi_2) = U_f(\sum_{x \in Z_2^n} \frac{|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \sum_{x \in Z_2^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Застосовуємо перетворення Уолша-Адамара до першого регістру та відкидаємо $n+1$ кубіт, після чого отримаємо квантову систему в стані $\psi_4 = \sum_{y \in Z_2^n} (\frac{1}{2^n} \sum_{x \in Z_2^n} (-1)^{f(x) \oplus x \cdot y}) |y\rangle = \sum_{y \in Z_2^n} \frac{S_f(y)}{2^n} |y\rangle$. Робимо вимірювання першого регістру. Для випадку коли $f(x) = a \cdot x$, фінальне вимірювання першого регістру поверне вектор a з ймовірністю 1.

Цей результат можна отримати за допомогою наступних міркувань. Перед фінальним вимірюванням першого регістру амплітуди квантових станів є коефіцієнтами Уолша-Адамара для функції f. Загальновідомо, що для лінійної функції її спектр має лише один ненульовий коефіцієнт, який і визначає лінійну структуру. Оскільки квадрати амплітуд дорівнюють ймовірності отримати стан, то єдина ненульова ймовірність буде для вектора a, тобто ймовірність отримати вектор a дорівнює $\|\frac{S_f(a)}{2^n}\|^2 = 1$. Цей алгоритм потребує $n+1$ кубіт та використовує один запит до оракула, інакше кажучи константну часову складність та лінійну просторову складність.

Недоліком цього алгоритму є те, що він застосовний тільки до одновимірних функцій, які є лінійними. Проте в роботах [5] та [13] його узагальнено на загальний випадок, з наведенням оцінок складності.

Для того, щоб розглянути даний алгоритм введемо деякі додаткові позначення. Нехай $N_f = \{\omega \in \{0,1\}^n : S_f(\omega) \neq 0\}$. Тоді справедлива наступна лема.

Лема 1.2. *Нехай дано функцію $f \in \mathfrak{B}_{n,1}$. Тоді для будь-якого $i \in \{0,1\}$ виконується співвідношення $U_f^i = \{a \in \{0,1\}^n : a \cdot \omega = i, \forall \omega \in N_f\}$.*

Дана лема дозволяє побудувати алгоритм знаходження лінійних конструкцій для функцій загального виду, який і був представлений в роботі [13], на який далі будемо посилатись як на узагальнений алгоритм Бернштейна-Вазірані.

Алгоритм 1.3. Узагальнений алгоритм Бернштейна-Вазірані

На вхід алгоритму подаємо f – функція з $\mathfrak{B}_{n,1}$, та N – число ітерацій алгоритму.

1) Покладемо $H = \{\}$ – порожня множина.

2) Для $i = 1..N$: застосувати алгоритм Бернштейна-Вазірані до функції f та додати результат його роботи до множини H.

3) Розв'язати системи лінійних рівнянь $\{x \cdot \omega = i \quad \omega \in H\}$ для $i = 0, 1$ та отримати розв'язки A^0 та A^1.

4) Якщо $A^0 \bigcup A^1 \subseteq \{0\}$ завершити роботу з помилкою, інакше повернути множину $A^0 \bigcup A^1$.

Повернені множини і будуть лінійними структурами функції f. В роботі [13] показано, що якщо функція f має не тривіальну лінійну структуру, тоді достатньо $O(n)$ ітерацій, для того, щоб зробити ймовірність помилки алгоритму як завгодно малою.

Наступним кроком буде побудова узагальнення даного алгоритму на випадок багатовимірної функції. Ідея даного узагальнення є дуже простою: знаходимо лінійні структури для кожної координатної функції, а потім беремо перетин цих множин.

Алгоритм 1.4. Узагальнений алгоритм Бернштейна-Вазірані для багатовимірної функції

На вхід алгоритму подаємо деяку багатовимірну функцію $F = (F_1, \ldots, F_m) \in \mathfrak{B}_{n,m}$, яка має лінійну структуру.

1) Для $i = 1..m$: знайти множину лінійних структур $A_i = A_i^0 \cup A_i^1$ для функції F_i за допомогою узагальненого алгоритму Бернштейна-Вазірані.

2) Обчислити результуючу множину $A = \bigcap_{i=1,m} A_i$.

3) Якщо $A \subseteq \{0\}$ завершити роботу з помилкою, інакше повернути A.

В роботі [13] доведено, що часова складність такого алгоритму дорівнює $O(nm)$, тобто, фактично, є квадратичною функцією довжини входу. При цьому алгоритм потребує $n + 1$ кубітів пам'яті.

1.4 Квантові атаки на основі обраного відкритого тексту на симетричні криптопримітиви

В більшості випадків квантові алгоритми Саймона та Бернштейна-Вазірані використовують з метою покращення класичних атак пошуку колізій. Зазвичай, шукане значення s – це значення

$s = E_k(\alpha) \oplus E_k(\beta)$ для деякої фіксованої пари значень $\alpha, \beta \in \{0,1\}^n$ та деякого відображення $E_k : \{0,1\}^n \longrightarrow \{0,1\}^n$.

Фактично, шукане значення s є періодом функції. Існують дві основні конструкції для побудови функції з певним періодом, які використовуються в квантовому криптоаналізі:

1) $f_1(x) = S(E_k(x) + E_k(x \oplus s))$

2) $f_2(x,b) = \delta_{b,0} E_k(x) + \delta_{b,1} E_k(x \oplus s)$

Нескладно перевірити, що період функції f_1 дорівнює s, а період функції f_2 дорівнює $s \| 1$. Отже, до функцій такого виду можна застосувати алгоритм Саймона для знаходження невідомого значення періоду.

Атака на трираундову мережу Фейстеля. Мережа Фейстеля – це класична ітеративна схема для побудови блокових шифрів. Вона була винайдена в 1973 році Хорстом Фейстелем і лягла в основу першого стандарту симетричного шифрування DES. Ця схема є ітеративним блоковим шифром в основі якої лежить раундова функція $F(x,k) = swap(x_l, f_k(x_l) \oplus x_r)$.

В роботі [14] доведено, що трираундова схема Фейстеля (рис. 1.2) є стійкою псевдовипадковою підстановкою в класичній моделі обчислень, проте пізніше в роботах [1] та [3] показано, що ця конструкція не є стійкою в квантовій моделі обчислень.

Твердження 1.1. *[1] [3]*

Трираундова мережа Фейстеля вразлива до атак розпізнавання в квантовій моделі обчислень.

Доведення.

Нехай $\alpha_0, \alpha_1 \in \{0,1\}^{n/2}$ – фіксовані повідомлення, n – довжина блоку шифрування в бітах, $(y_R, y_L) = E(\alpha_b, x)$ – повне шифруюче перетворення, $b \in \{0,1\}$.

Побудуємо функцію $f : \{0,1\}^n \times \{0,1\} \longrightarrow \{0,1\}^n$, яка визначається співвідношенням $f(x,b) = y_R \oplus \alpha_b = R_2(x \oplus R_1(\alpha_b))$, де $b \in \{0,1\}$. Періодом цієї функції є значення $s = R_1(\alpha_0) \oplus R_1(\alpha_1) \| 1$. Перевіримо це твердження.

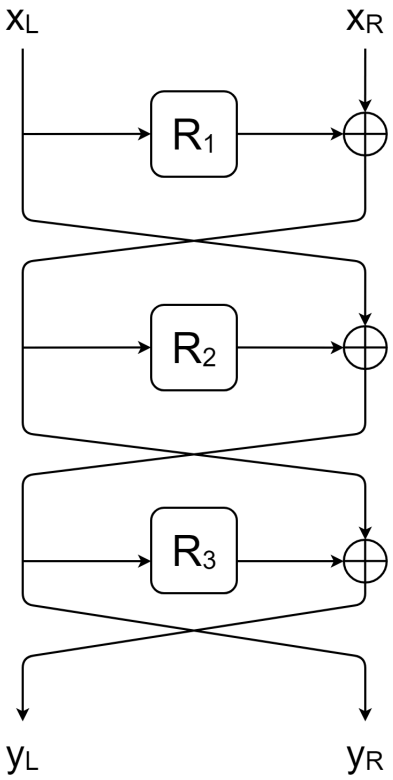

Рисунок 1.2 – Трираундова мережа Фейстеля

$$
\begin{gathered}
f(x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1), b \oplus 1) = \\
= R_2(x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1) \oplus R_1(\alpha_{b\oplus 1})) = \\
= R_2(x \oplus R_1(\alpha_0) \oplus R_1(\alpha_1) \oplus \delta_{b,0} R_1(\alpha_1) \oplus \delta_{b,1} R_1(\alpha_0)) = \\
= R_2(x \oplus \delta_{b,1} R_1(\alpha_1) \oplus \delta_{b,0} R_1(\alpha_0)) = \\
= R_2(x \oplus R_1(\alpha_b))
\end{gathered}
$$

Тож періодом цієї функції є значення $s = R_1(\alpha_0) \oplus R_1(\alpha_1)\|1$, отже, можна застосувати квантовий алгоритм Саймона для знаходження періоду цієї функції, що і буде безпосередньо атакою на таку мережу Фейстеля.

Для повноти атаки, розглянемо випадки коли $\epsilon(f, (R_1(\alpha_0) \oplus R_1(\alpha_1))\|1)$ менше та більше $\frac{1}{2}$. В випадку коли дана величина менше $\frac{1}{2}$ тоді відповідно до теореми наведеної раніше, можливо успішно використати алгоритм Саймона та знайти період побудованої конструкції. В випадку коли вона більше на $\frac{1}{2}$ – тоді до даної криптосистеми застосовні атаки методами диференціального криптоаналізу в класичній моделі обчислень. Тобто в обох випадках дана схема не є стійкою до атак розпізнавання. □

Атака на схему Івена-Мансура. Схема Івена-Мансура (рис. 1.3) була побудована в 1991 році, одним з основних застосувань якої є підсилення блокових шифрів. Вона має дуже просту структуру задану за допомогою наступного співвідношення: $E(x, k_1, k_2) = k_2 \oplus S(x \oplus k_1)$. В класичній моделі обчислень ця схема вважається криптографічно стійкою в загальному випадку, оскільки складність зламу потребує щонайменше $\Theta(2^{n/2})$ запитів до оракула. У квантовій моделі обчислень доведено її вразливість до атак на основі обраного відкритого тексту.[3]

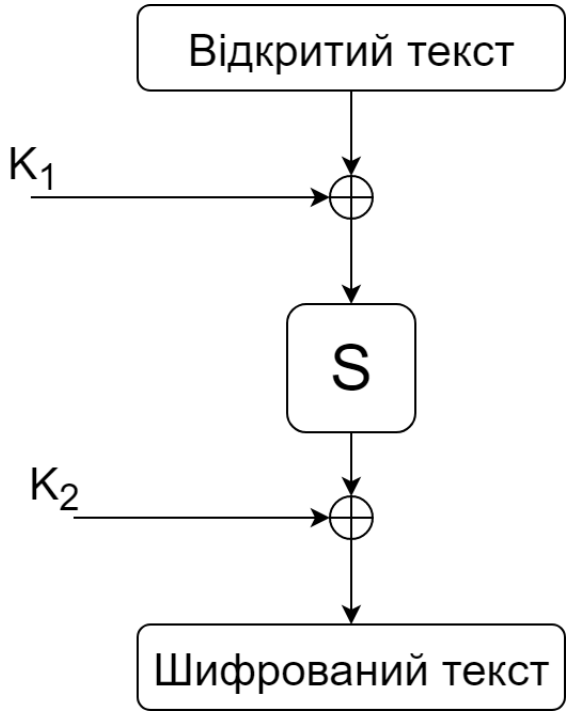

Рисунок 1.3 – Схема Івена-Мансура

Твердження 1.2. *Схема Івена-Мансура вразлива до квантових атак розпізнавання на основі обраного відкритого тексту. [3]*

Доведення.

Визначимо функцію $f(x) = E(x, k_1, k_2) \oplus S(x) = S(x \oplus k_1) \oplus S(x) \oplus k_2$. Очевидно, що ця функція має період k_1, який можна знайти за допомогою квантового алгоритму Саймона.

Аналогічно до атаки на трираундову мережу Фейстеля, розглянемо два випадки, в залежності від значення $\epsilon(f, k_1\|1)$ Якщо $\epsilon(f, k_1\|1) < \frac{1}{2}$ тоді

для такої функції f, алгоритм Саймона ефективно обчислить значення k_1, не зважаючи на наявність додаткових колізій. Якщо ж $\epsilon(f, k_1\|1) > \frac{1}{2}$, тоді існує атака розпізнавання класичній моделі обчислень, оскільки існуватиме деяке ненульове значення $t \neq k$ таке, що виконується нерівність $Pr[S(x) \oplus S(x \oplus k_1) \oplus S(x \oplus t) \oplus S(x \oplus k_1 \oplus t) = 0] > \frac{1}{2}$ □

Атака підробки повідомлення на код аутентифікації GMAC. Цей код аутентифікації повідомлень зроблено стандартом NIST в 2007 році. Вхідні повідомлення розглядаються як елементи деякого скінченного поля. В основі коду лежить конструкція Картера-Вегмана, яка й забезпечує криптографічну стійкість в класичній моделі обчислень.

Означення 1.6. Код аутентифікації GMAC

GMAC – код аутентифікації повідомлень, який визначається функцією $GMAC(N, M) = GHASH(M\|len(M)) \oplus E_k(N\|1)$, де $GHASH(M) = \sum_{i=0}^{len(M)} m_i \cdot H^{len(M)-i+1}$, $H = E_k(0)$, k – секретний ключ користувача, N – криптографічний нонс.

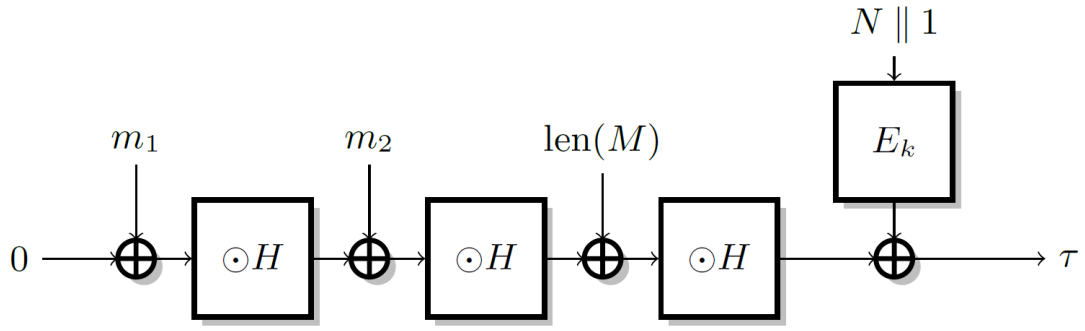

Рисунок 1.4 – Схема GMAC

Твердження 1.3. *Код аутентифікації повідомлень GMAC вразливий до атак підробки повідомлень в квантовій моделі обчислень. [3]*

Доведення.

Розглянемо повідомлення довжиною в два блоки $M = m_1\|m_2$. Тоді $GMAC(M, N) = \big((m_1 \cdot H) \oplus m_2\big) \cdot H \oplus E_k(N\|1)$. Нехай α_0 та α_1 деякі

фіксовані блоки. Для атаки побудуємо функцію $f_N : \{0,1\}^n \times \{0,1\} \longrightarrow \{0,1\}^n$, яка визначається співвідношенням $f_N(x,b) = GMAC(\alpha_b \| x, N) = \alpha_b \cdot H^2 \oplus x \cdot H \oplus E_k(N\|1)$, де $b \in \{0,1\}$. Тоді період функції f_N дорівнює $(\alpha_0 \oplus \alpha_1) \cdot H \| 1$

Покажемо це.

$$f_N(x \oplus (\alpha_0 \oplus \alpha_1) \cdot H, b \oplus 1) = GMAC(\alpha_{b\oplus 1} \| x \oplus (\alpha_0 \oplus \alpha_1) \cdot H, N) =$$
$$= \alpha_{b\oplus 1} \cdot H^2 \oplus (x \oplus (\alpha_0 \oplus \alpha_1) \cdot H) \cdot H \oplus E_k(N\|1) =$$
$$= \delta_{b,0}\alpha_1 \cdot H^2 \oplus \delta_{b,1}\alpha_0 \cdot H^2 \oplus x \cdot H \oplus (\alpha_0 \oplus \alpha_1) \cdot H^2 \oplus E_k(N\|1) =$$
$$= \delta_{b,0}\alpha_0 \cdot H^2 \oplus \delta_{b,1}\alpha_1 \cdot H^2 \oplus x \cdot H \oplus E_k(N\|1) =$$
$$= \alpha_b \cdot H^2 \oplus x \cdot H \oplus E_k(N\|1) = f(x,b)$$

Отже, до цієї функції можна застосувати алгоритм Саймона, для ефективного відновлення її періоду. Тоді код аутентифікації для випадкового фіксованого значення нонсу та довільного двоблокового повідомлення $m_1\|m_2$ буде також коректним для повідомлення $m_1 \oplus 1 \| m_2 \oplus H$ з тим самим значенням нонсу N. Ось це повідомлення $m_1 \oplus 1 \| m_2 \oplus H$ і буде підробкою оригінального повідомлення $m_1\|m_2$.

□

Важливо зазначити те, що як $GMAC$ так і f_N залежать від значення нонсу. Алгоритм Саймона на кожній ітерації має виконувати запит до оракула, який обчислює одну й ту саму функцію, проте кожна окрема ітерація алгоритму повертає вектор, ортогональний до вектора $((\alpha_0 \oplus \alpha_1) \cdot H)\|1$, який при цьому ніяк не залежить від вибору значення нонсу. Тож атака залишається коректною попри те, що на різних ітераціях алгоритму буде відбуватися запит до функції з різним нонсом.[3]

Атака раундового зсуву. Атаки раундового зсуву (англ. *slide attacks*) вперше описані в 1999 в роботі [15] Бірюкова та Вагнера. Вони можуть бути застосовані до класу блокових шифрів з ідентичним раундовим перетворенням $R(x,k) = P(x \oplus k)$, параметризованого одним і тим же ключем, де $P(x)$ – безключова раундова функція.

В класичній моделі обчислень ідея атаки полягає в отриманні $\Theta(2^{n/2})$ пар відкритого тексту та шифрованого тексту. З високою ймовірністю серед

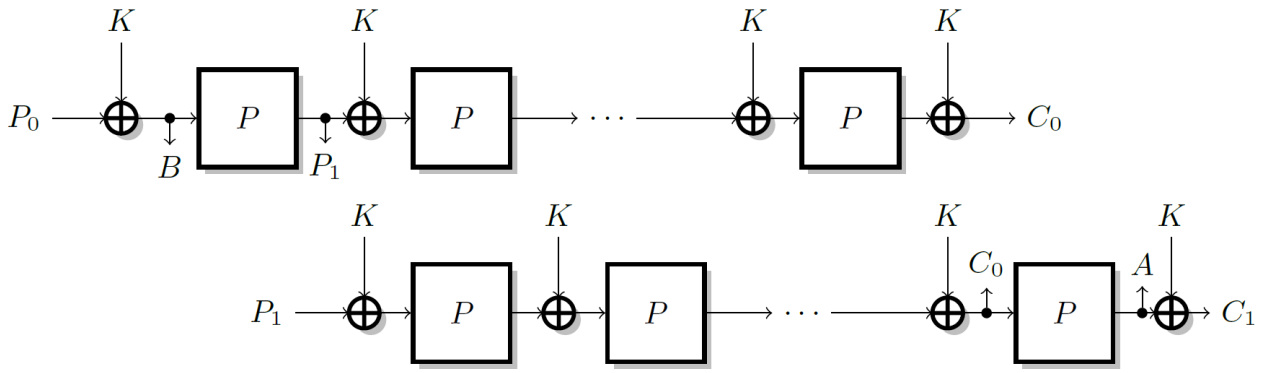

Рисунок 1.5 – Схема атаки раундового зсуву

цих пар знайдеться так звана «пара зсуву» – дві пари відкритого та шифрованого тексту (P_0, C_0) та (P_1, C_1) такі, що $R(P_0) = P_1$. Тоді для класу описаних вище шифрів одразу випливає: якщо пара повідомлень є парою зсуву, то $R(C_0) = C_1$ (рис. 1.5). В квантовій моделі обчислень можна отримати експоненційне зменшення складності цієї атаки.[3]

Твердження 1.4. *В квантовій моделі обчислень атака раундового зсуву потребує $O(n)$ запитів до оракула. [3]*

Доведення.

Нехай $P(x)$ – безключова раундова функція, $E_k(x)$ – повне шифруюче перетворення. Визначимо $f(x, b) = \delta_{b,0}(P(E_k(x)) \oplus x) \oplus \delta_{b,1}(E_k(P(x)) \oplus x)$. Не складно показати, що період функції f дорівнює $k\|1$. Застосувавши алгоритм Саймона до функції $f(x, b)$, ефективно знаходимо значення секретного ключа k. Відповідно до цього атака потребує $O(n)$ запитів до оракула, яка часова складність алгоритму Саймона. □

В роботі [3] доведено, що $\epsilon(f, k\|1) < \frac{1}{2}$, якщо перетворення $E_k \circ P$ та $P \circ E_k$ не відрізняються від випадкових підстановок. В цьому випадку атака суперпозиції дозволить ефективно відновити значення ключа k. Якщо ж $\epsilon(f, k\|1) > \frac{1}{2}$, то існує диференціал для перетворень $E_k \circ P$ та $P \circ E_k$ з ймовірністю, більшою за $\frac{1}{2}$.

1.5 Узагальнені мережі Фейстеля

Основна ідея, яка лежить в конструкції узагальнених мереж Фейстеля дуже проста – збільшити кількість блоків та задати структуру нелінійних перетворень і зсувів блоків повідомлення. В роботі розглянуті чотири популярні схеми для побудови блокових шифрів на основі мережі Фейстеля – це узагальнені мережі Фейстеля типу 1, 2, 3, які були представлені вперше в 1989 в роботі [16], а також незбалансовану мережу Фейстеля. Детальний аналіз цих конструкцій проведено в роботі [17].

Означення 1.7. Узагальнена мережа Фейстеля типу 1

Узагальненою мережею Фейстеля типу 1 (рис. 1.6) називається ітеративний блоковий шифр з раундовим перетворенням виду $F_k(x_0, x_1, x_2, x_3) = (x_1 \oplus R_k(x_0), x_2, x_3, x_0)$, де $R_k(x)$ – деяке невідоме перетворення на секретному ключі.

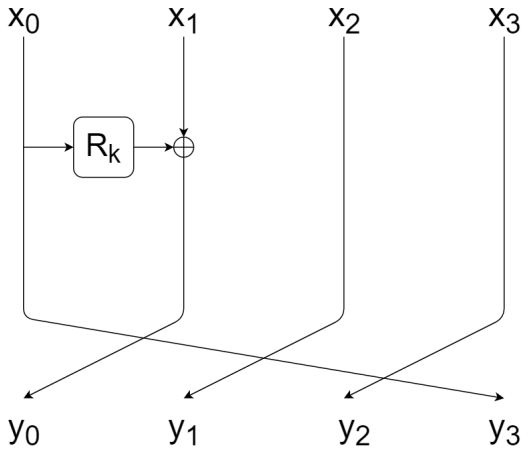

Рисунок 1.6 – Узагальнена мережа Фейстеля типу 1

Означення 1.8. Узагальнена мережа Фейстеля типу 2

Узагальненою мережею Фейстеля типу 2 (рис. 1.7) називається ітеративний блоковий шифр з раундовим перетворенням виду $F_k(x_0, x_1, x_2, x_3) = (x_1 \oplus R_k(x_0), x_2, x_3 \oplus R_k(x_2), x_0)$, де $R_k(x)$ – деяке невідоме перетворення на секретному ключі.

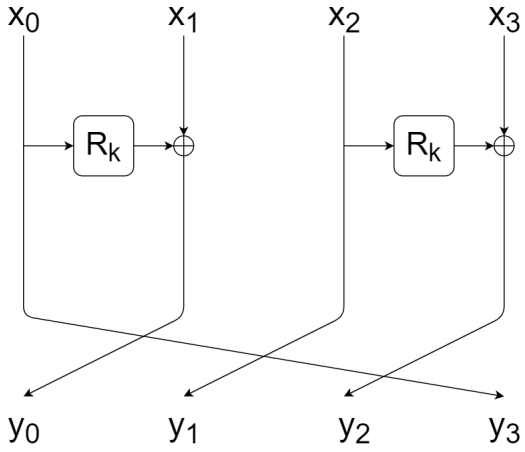

Рисунок 1.7 – Узагальнена мережа Фейстеля типу 2

Означення 1.9. Узагальнена мережа Фейстеля типу 3

Узагальненою мережею Фейстеля типу 3 (рис. 1.8) називається ітеративний блоковий шифр з раундовим перетворенням виду $F_k(x_0, x_1, x_2, x_3) = (x_1 \oplus R_k(x_0), x_2 \oplus R_k(x_1), x_3 \oplus R_k(x_2), x_0)$, де $R_k(x)$ – деяке невідоме перетворення на секретному ключі.

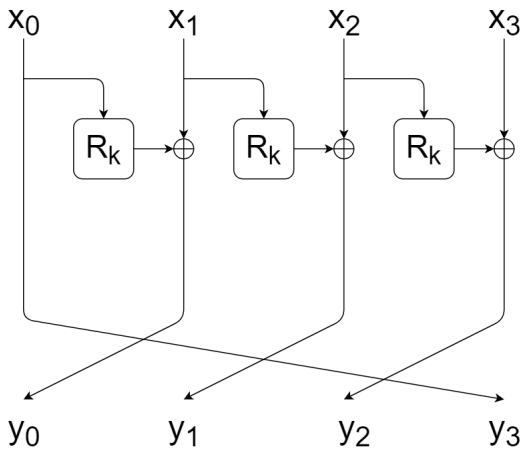

Рисунок 1.8 – Узагальнена мережа Фейстеля типу 3

Означення 1.10. Незбалансована мережа Фейстеля

Незбалансованою мережею Фейстеля (рис. 1.9) називається блоковий ітеративний шифр з блоком довжини n, раундове перетворення якого має вид $F_i(x_l, x_r) = (x_r, R_i(x_r) \oplus x_l)$, де x_l – блок довжини v, x_r – блок довжини u, за умови, що $v + u = n$, функція $R_i(\cdot)$ – деяке перетворення на секретному

ключі, яке діє з простору $\{0,1\}^u$ в простір $\{0,1\}^v$.

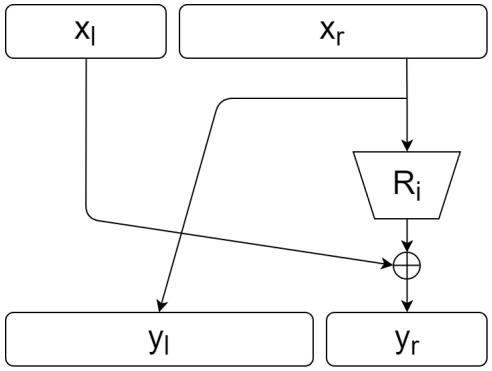

Рисунок 1.9 – Незбалансована мережа Фейстеля

Висновки до розділу 1

В розділі розглянуто необхідні теоретичні відомості з теорії квантових обчислень. З'ясовано чому квантові алгоритм Саймона та Бернштейна-Вазірані є одними з найперспективніших алгоритмів для використання в диференціальному криптоаналізі. Розглянуто задачі, що розв'язують ці алгоритми. Алгоритм Саймона за $\mathcal{O}(n)$ запитів до оракула розв'язує задачу пошуку періоду функції, де n довжина аргументу функції, тоді як алгоритм Бернштейна-Вазірані розв'язує задачу пошуку лінійної конструкції за $\mathcal{O}(n^2)$ запитів, де n довжина аргументу функції. Ці алгоритми потребують експоненційно меншої кількості кроків, ніж будь-який класичний алгоритм розв'язку таких задач. Узагальнення формулювання задачі Саймона на випадок функції з додатковими колізіями показує, що алгоритм Саймона може працювати з класом функцій, які майже задовольняють вимогам оригінальної задачі відповідно до метрики $\epsilon(f,s)$. Наявність додаткових колізій незначним чином впливає на роботу алгоритму, або до даної функції є застосовними методи класичного диференціального криптоаналізу. Розглянуто атаки з використанням

алгоритму Саймона на сучасні симетричні криптопримітиви такі як трираундова схема Фейстеля, схема Івена-Мансура, код аутентифікації повідомлень GMAC та пришвидшення класичної атаки раундового зсуву в експоненційну кількість кроків.

2 РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

В розділі представлено аналіз часової складності алгоритму Саймона та отримано ймовірнісні характеристики його роботи. Також узагальнено задачу Саймона на більші класи функцій, ніж ті, які описані в оригінальному формулюванні, перевірено можливість використання цих узагальнень до криптоаналізу мереж Фейстеля. Досліджено часові та ймовірнісні характеристики їх роботи.

Основна частина присвячена побудові атак на узагальнені мережі Фейстеля типів 1, 2, 3 та незбалансовану мережу Фейстеля, проведенню аналізу складності цих атак за допомогою вже відомих методів аналізу атак на основі алгоритмів Саймона та Бернштейна-Вазірані та оцінок, які будуть представлені в цьому розділі. Досліджено випадок атаки на криптопримітиви, що використовують мережу Фейстеля, як свою основну складову.

Далі будуть розглядатись квантові атаки на основі обраного відкритого тексту. Це означає, що квантовий супротивник має можливість обчислювати криптопримітив, який задано за допомогою оракула, від аргументу, що може знаходитись в стані квантової суперпозиції.

2.1 Аналіз квантового алгоритму Саймона для оригінального формулювання задачі

Аналіз квантового алгоритму Саймона є важливим аспектом цієї роботи, оскільки більшість атак як будуть представлені далі є прямим використанням цього алгоритму, тож матимуть такі самі ймовірнісні, часові та просторові характеристики роботи. Для його аналізу в більшості будуть використані методи теорії ймовірності, в наслідок ймовірнісної природи

даного алгоритму.

Доцільно почати аналіз алгоритму з доведення леми, яка використовувалась для отримання оцінки помилки узагальненого алгоритму Саймона. Дане доведення є простішим та використовує лише прямі переходи при доведенні, ніж те, що було представлене в оригінальній роботі [3].

Лема 2.1. *Нехай* $t \in \{0,1\}^n$. *Визначимо функцію* $g_t(x) = 2^{-n}\sum_{y\cdot t=0}(-1)^{x\cdot y}$ *для фіксованого* t. *Тоді* $g_t(x) = \frac{1}{2}(\delta_{x,0} + \delta_{x,t})$

Доведення.

Для доведення даної леми проведемо еквіваленті перетворення суми $\sum_{y\cdot t=0}(-1)^{x\cdot y} = 2^n g(x)$.

$$\begin{gathered}2^n g(x) = \textstyle\sum_{y\cdot t=0}(-1)^{x\cdot y} = \sum_y (1 - y\cdot t)(-1)^{x\cdot y} = \\ = \textstyle\sum_y (-1)^{x\cdot y} - \sum_y y\cdot t(-1)^{x\cdot y} = \\ = 2^n\delta_{x,0} + \textstyle\sum_y (-y\cdot t)(-1)^{x\cdot y} = \\ = 2^n\delta_{x,0} + \textstyle\sum_y (-1)^{y\cdot t}(-1)^{y\cdot x} - \sum_{y\cdot t=0}(-1)^{x\cdot y} = \\ = 2^n\delta_{x,0} + 2^n\delta_{x,t} - 2^n g(x)\end{gathered}$$

Розв'яжемо останнє співвідношення відносно $g(x)$.

$$\begin{gathered}2^n\delta_{x,0} + 2^n\delta_{x,t} - 2^n g(x) = 2^n g(x) \\ 2^n\delta_{x,0} + 2^n\delta_{x,t} = 2^n g(x) + 2^n g(x) \\ 2^n\delta_{x,0} + 2^n\delta_{x,t} = 2^{n+1} g(x) \\ g(x) = \tfrac{1}{2^{n+1}}(2^n\delta_{x,0} + 2^n\delta_{x,t}) \\ g(x) = \tfrac{1}{2}(\delta_{x,0} + \delta_{x,t})\end{gathered}$$

□

Алгоритм Саймона є ймовірнісним алгоритмом, в наслідок того, що на кожній ітерації він повертає деяке випадкове значення. Для подальшого аналізу алгоритму доцільно дослідити, який розподіл мають ці значення. Наступне твердження показує який розподіл мають дані значення.

Твердження 2.1. *Кожна ітерація алгоритму Саймона повертає випадковий бітовий вектор* u *з множини* $\{x : x\cdot s = 0\}$, *який є незалежним від інших ітерацій.*

Доведення.

Оскільки кожної ітерації алгоритму, незалежно від інших ітерацій, ініціалізуємо регістри новими значеннями, тому значення, які повертаються кожною ітерацією, є незалежними – очевидний факт.

Покажемо тепер, що ті значення які повертаються, це ортогональні до вектора s бітові вектори, на яких задано рівноймовірний розподіл.

Перед фінальним вимірюванням першого регістру він перебуває в стані $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_y(-1)^{zy}(1+(-1)^{sy})\,|y\rangle$. Доцільно розглянути два випадки: випадок, коли $y\cdot s=1$, та випадок, коли $y\cdot s=0$. Розглянувши дані випадки, ми повністю опишемо всі амплітуди квантових станів перед фінальним вимірюванням.

Нехай $y\cdot s=1$. Тоді маємо наступне співвідношення $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_y(-1)^{zy}(1+(-1)^{sy})\,|y\rangle=\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}(-1)^{zy}(1+(-1)^1)=0$. Отже, ітерація алгоритму Саймона дійсно не повертає вектори u такі, що $u\cdot s=1$.

Нехай $y\cdot s=0$, тоді коефіцієнт при стані $|y\rangle$ дорівнює $\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_y(-1)^{zy}(1+(-1)^{sy})\,|y\rangle=\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}(-1)^{zy}(1+(-1)^0)=\frac{2}{\sqrt{2}}\frac{1}{\sqrt{2^n}}$. Знайдемо квадрат норми цього коефіцієнта, який описує ймовірність отримати цей стан після вимірювання регістру. Тоді отримуємо $\|\frac{2}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\|^2=\frac{4}{2}\frac{1}{2^n}=2\frac{1}{2^n}=\frac{1}{2^{(n-1)}}$. Як бачимо, ці ймовірності описують рівноймовірний розподіл на множині $\{x:x\cdot s=0\}$, що й треба було довести. □

Маючи це твердження, можемо сформулювати твердження, про кількість кроків, необхідну для побудови системи векторів рангу $k+1$, з системи векторів рангу k. Використовуючи це маємо можливість, описати кількість кроків, яку зробить алгоритм Саймона, як суму випадкових величин, які описують кількість кроків для побудови системи більшого рангу, з системи меншого рангу.

Твердження 2.2. *Нехай n - розмірність векторного простору над полем F_2. Припустимо, що вже побудувано деяку систему з r векторів $\{u_{-r},\dots,u_{-1}\}$ рангу $k<n$, $\{u_i\}_{i=0}^{\infty}$ – деяка випадкова послідовність векторів з даного простору. Нехай випадкова величина*

$\xi_k = \min\{i \geq 0 : u_i \notin span(\{u_{-r}, \ldots, u_{-1}\})\}$. *Тоді випадкова величина* $\xi_k \sim Geom(1 - 2^{-n+k})$.

Доведення. Для доведення введемо послідовність випадкових величин $\eta_i = \delta_{u_i \notin span(\{u_{-r}, \ldots, u_{-1}\})}$. Тоді ці випадкові величини є незалежними, в наслідок незалежності u_i.

Тоді введемо нову випадкову величину $\xi_k = \min\{i \geq 0 : \eta = 1\} = \min\{i \geq 0 : u_i \notin span(\{u_{-r}, \ldots, u_{-1}\})\}$. Очевидно, що дана випадкова величина має геометричний розподіл, якщо за невдачу взяти подію, що u_i належить лінійній оболонці побудованій над заданими векторами, а за успіх – u_i не належить лінійній оболонці.

Знайдемо ймовірність невдачі. Очевидно, що ця ймовірність дорівнюватиме відношенню розміру лінійної оболонки до кількості всіх векторів. Маємо $|span(\{u_{-r}, \ldots, u_{-1}\})| = 2^k$. Тоді ймовірність невдачі дорівнює 2^{-n+k}, відповідно ймовірність успіху – $1 - 2^{-n+k}$.

Отже, $\xi_k \sim Geom(1 - 2^{-n+k})$, що й потрібно було довести.

□

Зауваження. Випадкова величина ξ_k показує кількість векторів необхідну для побудови системи рангу $k + 1$, з деякої вже побудованої системи рангу k, не включаючи вектор, що збільшує ранг системи.

Тепер опишемо кількість ітерацій, яку робить алгоритм Саймона. Якщо запропонувати наступну процедуру побудови системи лінійних рівнянь алгоритму Саймона: якщо вектор збільшує ранг системи, додаємо його, інакше – відкидаємо, тоді маємо наступний опис часу роботи алгоритму Саймона.

Твердження 2.3. *Випадкова величина* $\zeta = \sum_{k=1}^{n-2} \xi_k + n - 1$ *описує кількість кроків, яку зробить алгоритм Саймона для побудови системи векторів рангу* $n - 1$*, де випадкові величини* $\xi_k \sim Geom(1 - 2^{-n+1+k})$ *та є незалежними.*

Зауваження. Через те, що алгоритм Саймона повертає вектори $u \cdot s = 0$, тоді в якості лінійного простору векторів, потрібно взяти лінійний

підпростір розмірності $n-1$, який визначається співвідношенням $x \cdot s = 0$, та відповідно змінити розподіли випадкових величин ξ_k

Зауваження. Оскільки при доведенні твердження про кількість кроків, для побудови системи векторів більшого рангу, префікс послідовності вже побудований, проте є довільним, то випадкові величини ξ_k є незалежними.

Тепер використовуючи це твердження, можемо отримати оцінки часової складності квантового алгоритму Саймона.

Наслідок 2.1. *Середня кількість кроків яку зробить алгоритм Саймона дорівнює* $n - 1 + \frac{2^{n-2}-1}{2^{n-2}} + \frac{1}{3} \cdot \frac{4^{n-2}-1}{4^{n-2}}$.

Доведення. Знайдемо математичне очікування випадкової величини ζ – кількості кроків для побудови системи рангу $n-1$.

$$
\begin{aligned}
E[\zeta] = E[\textstyle\sum_{k=1}^{n-2} \xi_k + n - 1] = \sum_{k=1}^{n-2} E[\xi_k] + n - 1 = \sum_{k=1}^{n-2} \frac{2^{-n+1+k}}{1-2^{-n+1+k}} + n - 1 = \\
= \textstyle\sum_{k=1}^{n-2} \frac{1}{2^{n-1-k}-1} + n - 1 = n - 1 + \sum_{k=1}^{n-2} \frac{1}{2^{n-1-k}} \frac{1}{1-\frac{1}{2^{n-1-k}}} = \\
= n - 1 + \textstyle\sum_{k=1}^{n-2} \frac{1}{2^{n-1-k}} (1 + \frac{1}{2^{n-1-k}} + O(\frac{1}{2^{2(n-1-k)}})) \approx \\
\approx n - 1 + \textstyle\sum_{k=1}^{n-2} \frac{1}{2^{n-1-k}} + \sum_{k=1}^{n-2} \frac{1}{2^{2(n-1-k)}} = \\
= n - 1 + \frac{1}{2^{n-1}} \textstyle\sum_{k=1}^{n-2} 2^k + \frac{1}{2^{2(n-1)}} \sum_{k=1}^{n-2} 2^{2k} = \\
= n - 1 + \frac{1}{2^{n-1}} \textstyle\sum_{k=1}^{n-2} 2^k + \frac{1}{4^{n-1}} \sum_{k=1}^{n-2} 4^k = \\
= n - 1 + \frac{1}{2^{n-1}} \frac{2^{n-2}-1}{2-1} \cdot 2 + \frac{1}{4^{n-1}} \frac{4^{n-2}-1}{4-1} \cdot 4 = n - 1 + \frac{2^{n-2}-1}{2^{n-2}} + \frac{1}{3} \cdot \frac{4^{n-2}-1}{4^{n-2}}
\end{aligned}
$$

□

Наслідок 2.2. *При* $n \longrightarrow \infty$, *середня кількість кроків асимптотично дорівнює* $O(n)$.

Наслідок 2.3. *Середнє квадратичне відхилення кількості кроків, які зробить алгоритм Саймона дорівнює* $2^{-n+2} \cdot (2^{n-2} - 1) + \frac{1}{3} \cdot 2^{-2n+5} \cdot (2^{2n-4} - 1)$.

Доведення.

Знайдемо дисперсію випадкової величини ζ.

$$
\begin{aligned}
Var[\zeta] = Var[\textstyle\sum_{k=1}^{n-2} \xi_k + n - 1] = Var[\sum_{k=1}^{n-2} \xi_k] = \sum_{k=1}^{n-2} Var[\xi_k] = \\
= \textstyle\sum_{k=1}^{n-2} \frac{2^{-n+1+k}}{(1-2^{-n+1+k})^2} = \sum_{k=1}^{n-2} 2^{-n+1+k} \cdot \left[\frac{1}{1-x}\right]'_{x=2^{-n+1+k}} =
\end{aligned}
$$

$$= \sum_{k=1}^{n-2} 2^{-n+1+k} \cdot \left[\sum_{i=0}^{\infty} x^i \right]'_{x=2^{-n+1+k}} = \sum_{k=1}^{n-2} 2^{-n+1+k} \cdot \left[\sum_{i=1}^{\infty} i \cdot x^{i-1} \right]_{x=2^{-n+1+k}} \approx$$
$$\approx \sum_{k=1}^{n-2} 2^{-n+1+k} \cdot (1 + 2 \cdot 2^{-n+1+k}) = \sum_{k=1}^{n-2} 2^{-n+1+k} + \sum_{k=1}^{n-2} 2 \cdot 2^{2(-n+1+k)} =$$
$$= 2^{-n+1} \sum_{k=1}^{n-2} 2^k + 2^{-2n+3} \sum_{k=1}^{n-2} 4^k = 2^{-n+1} \cdot \frac{2^{n-2}-1}{2-1} \cdot 2 + 2^{-2n+3} \cdot \frac{4^{n-2}-1}{4-1} \cdot 4 =$$
$$= 2^{-n+2} \cdot (2^{n-2} - 1) + \frac{1}{3} \cdot 2^{-2n+5} \cdot (2^{2n-4} - 1)$$

□

Наслідок 2.4. *Ймовірність того, що алгоритм Саймона не поверне системи рангу* $n - 1$ *прямує до нуля з ростом* n*, тобто* $\lim_{n \to +\infty} Pr[\zeta = +\infty] = 0$.

Отже, в результаті детального аналізу алгоритму Саймона методами теорії ймовірності, було підтверджено те, що цей алгоритм має лінійну часову складність. Знайдено точні оцінки для середньої кількості кроків, що зробить алгоритм, та середнє квадратичне відхилення кількості кроків від середньої кількості. Показано, що ймовірність того, алгоритм ніколи не поверне системи векторів рангу $n - 1$ прямує до нуля з ростом довжини входу функції, що подається на вхід алгоритму.

2.2 Задача Саймона з прихованим перетворенням аргументу

Як будо показано в роботі [3], алгоритм Саймона може коректно працювати з набагато більшим класом функцій. Це дає привід для подальших досліджень в узагальненні або розширенні формулювання задачі Саймона. Далі показано, що алгоритм Саймона не розрізняє функції, які пов'язані лише деякою бієктивною підстановкою.

Введемо нові позначення. Нехай Σ – множина всіх бієктивних функцій які діють з простору бітових векторів $\{0,1\}^n$ в простір бітових векторів $\{0,1\}^n$. Тоді очевидним є факт, що потужність цієї множини дорівнює $|\Sigma| = (2^n)!$ – як кількість перестановок вхідних векторів таблиці істинності, яка повністю визначає булеву функцію.

Розширимо формулювання задачі Саймона на випадок пари функцій, які пов'язані деяким бієктивним перетворенням аргументу.

Задача 2.1. Задача Саймона з прихованим перетворенням аргументу

Нехай задано функції $f : \{0,1\}^n \longrightarrow \{0,1\}^n$ та $g : \{0,1\}^n \longrightarrow \{0,1\}^n$ та відомо, що вони пов'язані співвідношенням $f(x) = g(\sigma(x))$, $\sigma(x) \in \Sigma$ – деяке невідоме бієктивне перетворення аргументу. Для довільних значень $x, y \in \{0,1\}^n$ рівність виконується $f(x) = f(y)$ тоді і тільки тоді, коли $(x \oplus y) \in \{0, s\}$, для деякого невідомого фіксованого значення $s \in \{0,1\}^n$. Необхідно визначити чи існує ненульове значення s та знайти його, маючи можливість обчислювати значення від суперпозиції тільки для функції g.

Твердження 2.4. *Якщо алгоритму Саймона подати на вхід подати функцію $g(x)$, то за $O(n)$ запитів він розв'яже задачу Саймона для функції $f(x)$.*

Доведення.

1) Підготувати два регістри розміру n у стані $|0\rangle\,|0\rangle$.

2) Застосувати перетворення Уолша-Адамара до першого регістру $(H^{\otimes n} \otimes I_n)\,|0\rangle\,|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in Z_2^n} |x\rangle\,|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in Z_2^n} |\sigma(x)\rangle\,|0\rangle$.

3) Використати стандартну модель оракулу, який обчислює значення функції g: $U_g(\frac{1}{\sqrt{2^n}} \sum_x |\sigma(x)\rangle\,|0\rangle) = \frac{1}{\sqrt{2^n}} \sum_x |\sigma(x)\rangle\,|g(\sigma(x))\rangle = \frac{1}{\sqrt{2^n}} \sum_t |t\rangle\,|f(t)\rangle$.

4) Зробити вимірювання другого регістру, що переведе перший регістр у стан $\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)$ для деякого значення z, де $f(z)$ є результатом вимірювання.

5) Застосувати перетворення Уолша-Адамара до першого регістру $H^{\otimes n}(\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)) = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_y (-1)^{zy}(1 + (-1)^{sy})\,|y\rangle$.

6) Зробити вимірювання першого регістру. Результатом вимірювання буде деяке випадкове значення $u \in \{0,1\}^n$ таке, що $u \cdot s = 0$.

Як тільки ранг системи рівнянь $u_i \cdot s = 0$ стане $n - 1$, розв'язуємо її та знаходимо значення s. □

Наслідок 2.5. *Алгоритм Саймона не розрізняє функції, які пов'язані*

лише деяким бієктивним перетворенням аргументу.

Це узагальнення дає можливість проводити атаки розпізнавання на функції, де приховане перетворення аргументу є деяким перетворенням на секретному ключі. Хоча супротивник не може робити запити до даного перетворення, завдяки цьому узагальненню він все одно має коректні атаки на основі алгоритму Саймона.

В наслідок дослідження даного узагальнення, було знайдено загальну властивість всіх квантових обчислень – при обчисленні функції від рівномірної суперпозиції аргументу, квантовий оракул не розрізняє функції пов'язані бієктивним перетворенням аргументу, тобто маємо відношення еквівалентності на множині функцій. Дві функції будуть еквівалентними відносно операції обчислення функції від рівномірної суперпозиції аргументу, тоді і тільки тоді, коли вони пов'язані деяким бієктивним перетворенням аргументу. Як наслідок при застосуванні операції обчислення функції від рівномірної суперпозиції аргументу до функцій з одного класу еквівалентності, в результаті отримуватимемо квантові системи в одному і тому ж самому стані.

2.3 Задача Саймона для функції з неповною колізією

В роботі [3] формулювання задачі Саймона було узагальнено на випадок коли функція має додаткові неповні колізії, тобто співвідношення $f(x) = f(x \oplus t)$ виконувалося тільки для деякої підмножини аргументів. Узагальнення, яке представлене в даному розділі, розглядає випадок коли, функція має лише неповну колізію.

Введемо додаткові поняття.

Означення 2.1. Вектор $t \in \{0,1\}^n$ будемо називати неповною колізією, якщо $\exists S \subset \{0,1\}^n$ – нетривіальна підмножина векторів, що $\forall x \in S : f(x) = f(x \oplus t)$. Тоді множину S будемо називати множиною

неповної колізії t.

Випадок коли $S = \{0,1\}^n$ будемо називати повною колізією, або ж просто – функцією з періодом, у термінах функцій.

Тепер переформулюємо задачу Саймона на випадок функції з неповною колізією.

Задача 2.2. Задача Саймона для функції з неповною колізією

Нехай дано функцію $f : \{0,1\}^n \longrightarrow \{0,1\}^n$, таку що $\exists S \subseteq \{0,1\}^n$ – нетривіальна підмножина векторів, що $\forall x \in S$ співвідношення $f(x) = f(y)$ виконується тоді і тільки тоді, коли $(x \oplus y) \in \{0, s\}$. $\forall x \in \{0,1\}^n \setminus S$ функція f визначена довільно. Задача знайти невідоме значення вектора s.

В цьому випадку алгоритм Саймона прямо не застосовний. Проте, як побачимо далі, при деяких додаткових умовах та процедурах з множиною векторів $\{u_i\}$ – результатів ітерацій алгоритму Саймона, супротивник має можливість відновити неповну колізію s. Для цього спочатку розглянемо наступне твердження.

Твердження 2.5. *Ітерація алгоритму Саймона для випадку функції з неповною колізією, повертає вектор ортогональний до вектора неповної колізії s або деяке випадкове значення, відповідно до деякого ймовірнісного розподілу.*

Доведення.

Нехай дано функцію $f \in \mathfrak{B}_{n,n}$, яка має неповну колізію s на нетривіальній множині $S \subset \{0,1\}^n$. Розглянемо як ітерація алгоритму Саймона відпрацює на цій функції.

1) Підготувати два регістри розміру n у стані $|0\rangle |0\rangle$.

2) Застосувати перетворення Уолша-Адамара до першого регістру $(H^{\otimes n} \otimes I_n) |0\rangle |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in Z_2^n} |x\rangle |0\rangle$.

3) Використати стандартну модель оракулу, який обчислює значення функції f: $U_f(\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |0\rangle) = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$.

4) Зробити вимірювання другого регістру.

Нехай результатом вимірювання регістру є значення $\gamma \in Im[f]$. Це переведе перший регістр у стан $\delta_{\gamma \in Im[f](S)}(|z\rangle + |z \oplus s\rangle) + \sum_{t \notin S, f(t)=\gamma} |t\rangle$, де $f(z) = \gamma$ для деякого $z \in S$.

Тоді доцільно розглянути два випадки $\gamma \in Im[f](\{0,1\}^n \setminus S)$ та $\gamma \notin Im[f](\{0,1\}^n \setminus S)$.

Якщо $\gamma \notin Im[f](\{0,1\}^n \setminus S)$, тоді перший регістр перебуває в стані $(|z\rangle \oplus |z \oplus s\rangle)$, де $f(z) = \gamma$. Тоді подальше виконання алгоритму Саймона поверне коректний вектор u_i такий, що $u_i \cdot s = 0$.

Якщо $\gamma \in Im[f](\{0,1\}^n \setminus S)$, тоді перший регістр перебуває в деякому стані $\delta_{\gamma \in Im[f](S)}(|z\rangle + |z \oplus s\rangle) + \sum_{t \notin S, f(t)=\gamma} |t\rangle$. При подальшому виконанні, застосування перетворення Уолша-Адамара до першого регістру переведе його в деякий довільний стан, і після виміру першого регістру отримаємо деяке випадкове значення.

В результаті послідовних ітерації, алгоритм Саймона поверне систему векторів, в якій є як вектори ортогональні до вектора s, так і ті, що не є ортогональними до вектора s. □

Наслідок 2.6. *Ітерація алгоритму Саймона повертає ортогональні та не ортогональні до вектора s вектори відповідно до розподілу Бернуллі, параметр якого залежить від розміру множини S та структури функції f.*

Наслідок 2.7. *Алгоритм Саймона для функції з неповною колізією поверне систему векторів відповідно до біноміального розподілу з параметром «успіху» (отримати ортогональний вектор) визначеним вище в розподілі Бернуллі.*

В найгіршому випадку, коли отримали значення другого регістру $\gamma \in Im[f](\{0,1\}^n \setminus S)$, після виміру першого регістру завжди отримуватимемо не ортогональні вектори $u_i \cdot s = 1$. Необхідно знайти оцінку ймовірності того, що ітерація алгоритму Саймона поверне некоректний вектор. Наступне твердження наводить цю оцінку.

Твердження 2.6. *Ймовірність того, що ітерація алгоритму*

Саймона для функції f з неповною колізією поверне некоректний вектор не більша ніж $\frac{3(2^n-|S|)}{2^n}$.

Доведення.

Ймовірність того, що ітерація алгоритму поверне некоректний вектор визначається потужністю множини $Im[f](\{0,1\}^n \setminus S)$ та структурою функції f, а саме множиною $Im[f](S) \bigcap Im[f](\{0,1\}^n \setminus S)$.

$$p_{fail} = \sum_{\gamma \in Im[f]} p_{fail}^{\gamma} Pr_x[f(x) = \gamma] =$$
$$= \sum_{\gamma \in Im[f](F_2^n \setminus S)} p_{fail}^{\gamma} Pr_x[f(x) = \gamma] + \sum_{\gamma \in Im[f] \setminus Im[f](F_2^n \setminus S)} p_{fail}^{\gamma} Pr_x[f(x) = \gamma] =$$
$$= \sum_{\gamma \in Im[f](F_2^n \setminus S)} p_{fail}^{\gamma} Pr_x[f(x) = \gamma] \leq \sum_{\gamma \in Im[f](F_2^n \setminus S)} Pr_x[f(x) = \gamma] =$$
$$= \frac{1}{2^n} \sum_{\gamma \in Im[f](F_2^n \setminus S)} \#\{x | f(x) = \gamma\} \leq \frac{3(2^n - |S|)}{2^n}$$

□

Принципіальною відмінністю розв'язку цієї задачі від оригінальної задачі Саймона є те, що в результаті роботи алгоритм повертає систему векторів, в якій є некоректні вектори. Тому додатково постає задача обробки такої системи.

Можливі два основні шляхи роботи з такою системою: відфільтрувати некоректні вектори або використати методи теорії розв'язку рівнянь з спотвореною правою частиною. Ефективність алгоритму повністю визначається, тим наскільки ефективно можна опрацювати систему векторів з некоректними векторами. Наведемо декілька евристик, які можна використати для ефективного алгоритму фільтрування.

Твердження 2.7. *Якщо $\{u_{i_j}\}$ підсистема рангу $n-1$, яка складається тільки з коректних векторів, тоді додавання будь-якого не коректного вектора збільшує ранг системи до n.*

Твердження 2.8. *Якщо $1 - \frac{|S|}{2^n} << \frac{1}{2}$, тоді система векторів $\{u_i\}$ є сильно незбалансованою, тобто кількість коректних векторів значно більша ніж не коректних.*

На основі цих евристик запропонуємо алгоритм для розв'язку задачі фільтрації.

Алгоритм 2.1. Алгоритм фільтрації системи векторів

На вхід алгоритму подається система векторів $U = \{u_i\}_{i=0}^{N}$ та деяке число $M > 0$.

1) Ініціалізувати $Q = \{\}$.

2) Для j від 1 до M: згенерувати випадкову систему векторів $q_j \subset U$ рангу $n-1$ та додати її до множини Q.

3) Ініціалізувати $c[M] = [0, \ldots, 0]$ – масив лічильників довжини M, асоційований з системами q_i.

4) Для всіх $u \in U \setminus (\bigcup q_i)$ та $q_i \in Q$: якщо ранг системи векторів $rang(q_i \bigcup u) = n$, тоді збільшити лічильник $c[i]$ на одиницю.

5) Повернути систему векторів q_i, для якої лічильник мінімальний.

Алгоритм повертає деяку систему векторів q_i рангу $n-1$. Розв'язавши відповідну систему лінійних рівнянь отримуємо невідоме значення s та робимо ймовірнісну перевірку коректності результату.

Розглянемо чому цей алгоритму поверне систему векторів, що ортогональні до вектора s. Розглянемо три випадки: система векторів $q_i \in Q$ складається тільки з ортогональних до s векторів, тільки з не ортогональних до s векторів, та останній випадок – в системі присутні як ортогональні, так і не ортогональні вектори. Далі будемо суттєво користуватись евристиками, що були наведені вище, а саме ти, що система векторів U є сильно не збалансованою.

Якщо система складалась тільки з ортогональних векторів, то при додаванні кожного не ортогонального вектора, ранг буде збільшуватись, а при додаванні ортогонального – змінюватись не буде. Отже, лічильник для такої системи дорівнюватиме кількості не ортогональних до s векторів, що належать системі $U \setminus (\bigcup q_i)$.

Аналогічно для системи, що складається тільки з не ортогональних векторів, лічильник для такої системи буде дорівнювати, кількості ортогональних до вектора s векторів в системі векторів $U \setminus (\bigcup q_i)$. Для випадку змішаної системи, лічильник матиме деяке значення, не менше за лічильник для системи ортогональних векторів, та не більше за лічильник

для системи не ортогональних векторів. При цьому в наслідок того, що система векторів U є незбалансованою, то лічильник для системи ортогональних векторів буде меншим, за лічильник для системи не ортогональних векторів.

Тому, якщо система векторів достатньо не збалансована, то в множині Q знайдеться така система векторів, що складається тільки, з ортогональних векторів, яку й поверне цей алгоритм.

Дослідимо наскільки не збалансованою має бути система.

Якщо розглянути нескінченну послідовність векторів, що є результом роботи алгоритму Саймона для функції з неповною колізією, тоді можна ввести випадкову величину ϕ кількості ортогональних векторів до першого неортогонального. Ця випадкова величина матиме геометричний розподіл з параметром «успіху» $p \leq p_{fail} = \frac{3(2^n - |S|)}{2^n}$. Випадкова перестановка векторів не змінює розподілу, оскільки ітерації алгоритму незалежні.

Приблизимо розподіл скінченної системи векторів отриманої в результаті роботи алгоритму Саймона визначенним вище розподілом нескінченної послідовнотсі з достатньою точністю. Тоді процедура побудови випадкової системи рангу $n-1$ зводиться до перемішування всієї системи векторів та побудови системи методом послідовного додавання векторів до системи доки її ранг не стане $n-1$.

Як було отримано вище, середня кількість кроків алгоритму Саймона для оригінальної задачі для побулови системи рангу $n-1$ є лінійною та значно меншою ніж $2n$. Тоді, якщо $Pr[\phi > 2n] > \frac{1}{2}$, то відповідно ймовірність, що в множині Q не буде жодної системи тільки з ортогональних векторів буде не більша ніж 2^{-M}. Тобто, її достатньо швидко можна зробити, як завгодно малою.

Знайдемо для якої потужнотсі множини S це виконується. Розглянемо ймовірність $Pr[\phi > 2n] = \sum_{i=2n}^{+\infty}(1-p)^i p = (1-p)^{2n}\sum_{i=0}^{+\infty}(1-p)^i p =$
$= (1-p)^{2n} \geq (1-p_{fail})^{2n} = \frac{1}{2}$.

Розв'язуємо останнє співвідношення відносно p_{fail} та отримуємо $p_{fail} = 1 - 2^{-\frac{1}{2n}}$. Тоді, враховуючи значення p_{fail} отримане вище, отримуємо

наступну оцінку для потужності $|S| = \frac{2}{3}2^n + \frac{1}{3}2^{-n}$. Тобто, це означає, що якщо потужність множини S є не меншою від двох третіх від кількості всіх векторів, то алгоритм фільтарації поверне систему, що складається тільки з ортогональних векторів, з ймовірністю як завгодно близькою до одниці.

Значним недоліком цього алгоритму є те, що його робота значним чином опирається на незбалансованість системи векторів U, що в свою чергу зменшує область його застосування.

Це узагальнення алгоритму Саймона дає змогу працювати з набагато більшим класом функцій, ніж дає змогу оригінальне формулювання задачі. Проте значним недоліком цього узагальнення є додаткова обробка системи векторів з не коректними значеннями, від ефективності якої значним чином залежить ефективність всього алгоритму.

2.4 Атаки розпізнавання на узагальнену мережу Фейстеля типу 1

Як було розглянуто раніше, трираундова мережа Фейстеля не є стійкою псевдовипадковою підстановкою в квантовій моделі обчислень. Це є причиною дослідження узагальнених мереж Фейстеля на вразливість до атак такого виду.

Узагальнена мережа Фейстеля типу 1 є найпростішим узагальненням мережі Фейстеля. За один раунд шифрування значних нелінійних змін зазнає лише один блок, перетворення інших блоків є простим зсувом. Це створює значні вразливості цієї конструкції до атак на основі квантових алгоритмів Саймона та Бернштейна-Вазірані.

В цьому розділі будуть представлені дві атаки на цю конструкцію. Перша атака це узагальнення атаки на звичайну мережу Фейстеля представленої в роботі [3]. Друга атака є значним покращенням першої з використанням алгоритму Бернштейна-Вазірані.

Проведемо узагальнення атаки представленої в роботі [3]. Для простоти викладки розглянемо цю атаку на основі чотириблокової узагальненої мережі Фейстеля типу 1, а потім узагальнимо цю атаку на довільну кількість блоків d.

В основі даної атаки лежить той факт, що після раунду шифрування, більшість блоків є простим зсувом.

Твердження 2.9. *Семираундова узагальнена мережа Фейстеля типу 1 є вразливою до квантових атак розпізнавання на основі обраного відкритого тексту.*

Доведення.

Побудуємо атаку на семираундову узагальнену мережу Фейстеля типу 1.

Для цього розглянемо перший блок шифротексту y_1. Він має вид $x_0 \oplus R_4(x_3 \oplus R_3(x_2 \oplus R_2(x_1 \oplus R_1(x_0))))$. Структура блоку є такою самою, як і відповідній атаці для звичайної мережі Фейстеля, тож використаймо стандарту методику побудови атаки представлену раніше.

Нехай $\alpha_0 = (\alpha_0^{(0)}, \alpha_0^{(1)}, \alpha_0^{(2)})$ та $\alpha_1 = (\alpha_1^{(0)}, \alpha_1^{(1)}, \alpha_1^{(2)})$, $\alpha_0 \neq \alpha_1$ – фіксовані повідомлення, $E_k(x_0, x_1, x_2, x_3) = (y_0, y_1, y_2, y_3)$ – повне шифруюче перетворення.

Визначимо функцію $f(x, b) = \left[E_k(\alpha_b^{(0)}, \alpha_b^{(1)}, \alpha_b^{(2)}, x)\right]_{y_1} \oplus \alpha_b = y_1 \oplus \alpha_b^{(0)} =$
$= \alpha_b^{(0)} \oplus R_4(x \oplus R_3(\alpha_b^{(2)} \oplus R_2(\alpha_b^{(1)} \oplus R_1(\alpha_b^{(0)})))) \oplus \alpha_b^{(0)} =$
$= R_4(x \oplus R_3(\alpha_b^{(2)} \oplus R_2(\alpha_b^{(1)} \oplus R_1(\alpha_b^{(0)}))))$, де індекс $b \in \{0, 1\}$.

Позначимо через $G(x_0, x_1, x_2) = R_3(x_2 \oplus R_2(x_1 \oplus R_1(x_0)))$. Тоді період функції $f(x, b)$ дорівнює $(G(\alpha_0) \oplus G(\alpha_1))\|1$.

Дійсно, $f(x, b) \oplus f(x \oplus G(\alpha_0) \oplus G(\alpha_1), b \oplus 1) = R_4(x \oplus G(\alpha_b)) \oplus$
$\oplus R_4(x \oplus G(\alpha_0) \oplus G(\alpha_1) \oplus G(\alpha_{b\oplus 1})) = R_4(x \oplus G(\alpha_b)) \oplus R_4(x \oplus G(\alpha_b)) = 0$.

Отже, квантовий алгоритм Саймона ефективно відновлює значення $s = (G(\alpha_0) \oplus G(\alpha_1))\|1$ періоду функції f та розпізнає цю конструкцію. □

На основі даного прикладу можемо побудувати загальну атаку для узагальненої мережі Фейстеля типу 1 з довільною кількістю блоків d.

Раундове перетворення такої мережі має вигляд $F_i(x_0, \ldots, x_{d-1}) = (x_1 \oplus R_i(x_0), x_2, x_3, \ldots, x_{d-1}, x_0)$. Тоді маємо наступне твердження.

Твердження 2.10. *$(2d-1)$-раундова узагальнена мережа Фейстеля типу 1 вразлива до квантових атак розпізнавання на основі обраного відкритого тексту.*

Доведення.

Побудуємо атаку розпізнавання на $(2d-1)$-раундову узагальнену мережу Фейстеля типу 1 з кількістю блоків d.

Нехай $\alpha_0 = (\alpha_0^{(0)}, \ldots, \alpha_0^{(d-2)})$ та $\alpha_1 = (\alpha_1^{(0)}, \ldots, \alpha_1^{(d-2)})$, $\alpha_0 \neq \alpha_1$ – фіксовані повідомлення, $E_k(x_0, \ldots, x_{d-1}) = (y_0, \ldots, y_{d-1})$ – повне шифруюче перетворення.

Перший блок шифрування y_1 має вид $x_0 \oplus R_d(x_{d-1} \oplus R_{d-1}(x_{d-2} \oplus \ldots \oplus R_2(x_1 \oplus R_1(x_0))))$.

Відповідно до атаки розглянутої раніше, визначимо функцію $f(x,b) = \left[E_k(\alpha_b^{(0)}, \ldots, \alpha_b^{(d-2)}, \alpha_b^{(2)}, x)\right]_{y_1} \oplus \alpha_b = y_1 \oplus \alpha_b^{(0)} =$
$= \alpha_b^{(0)} \oplus R_d(x \oplus R_{d-1}(\alpha_b^{(d-2)} \oplus \ldots \oplus R_2(\alpha_b^{(1)} \oplus R_1(\alpha_b^{(0)})))) \oplus \alpha_b^{(0)} =$
$= R_d(x \oplus R_{d-1}(\alpha_b^{(d-2)} \oplus \ldots \oplus R_2(\alpha_b^{(1)} \oplus R_1(\alpha_b^{(0)})))$, де індекс $b \in \{0,1\}$.

Позначимо через $G(x_0, x_1, \ldots, x_{d-2}) = R_{d-1}(x_{d-2} \oplus \ldots \oplus R_2(x_1 \oplus R_1(x_0)))$

Аналогічно до Тоді період такої функції $f(x,b)$ дорівнює $(G(\alpha_0) \oplus G(\alpha_1)) \| 1$.

$f(x,b) \oplus f(x \oplus G(\alpha_0) \oplus G(\alpha_1), b \oplus 1) = R_4(x \oplus G(\alpha_b)) \oplus$
$\oplus R_4(x \oplus G(\alpha_0) \oplus G(\alpha_1) \oplus G(\alpha_{b \oplus 1})) = R_4(x \oplus G(\alpha_b)) \oplus R_4(x \oplus G(\alpha_b)) = 0$

Значення цього періоду ефективно знаходиться за допомогою квантового алгоритму Саймона. □

Твердження 2.11. *Атака на $(2d-1)$-раундову узагальнену мережу Фейстеля типу 1 має часову складність $O(\frac{n}{d})$ та потребує $(\frac{2n}{d} + 1)$ кубітів, де n – довжина блоку шифрування криптопримітиву E_k в бітах, d – кількість блоків.*

Доведення.

Оскільки атака зводиться до використання квантового алгоритму Саймона до функції f, то весь аналіз, який був проведений для алгоритму Саймона залишається справедливим і для цієї атаки. □

В ході дослідження було з'ясовано, що ця атака не є найкращою у випадку коли супротивник має доступ до шифруючого оракула. Наступна атака опиратиметься на той факт, що якщо зафіксувати $d-2$ блоків довільними константами і варіювати індексом b лише один передостанній блок то кількість раундів, які супротивник може розпізнати зросте в лінійну кількість разів. Це демонструє наступна атака.

Твердження 2.12. *Десятираундова узагальнена мережа Фейстеля типу 1 є вразливою до квантових атак розпізнавання на основі обраного відкритого тексту.*

Доведення.

Побудуємо атаку на десять раундів узагальненої мережі Фейстеля типу 1.

Нехай $\gamma_0 = (\alpha^{(0)}, \alpha^{(1)}, \beta_0)$ та $\gamma_1 = (\alpha^{(0)}, \alpha^{(1)}, \beta_1)$, $\beta_0 \neq \beta_1$ – фіксовані повідомлення. Тобто визначимо вектори в яких перші два блоки є однаковими, а останні – відрізняються. $E_k(x_0, x_1, x_2, x_3) = (y_0, y_1, y_2, y_3)$ – повне шифруюче перетворення.

Другий блок шифротексту має вид $y_1 = x_3 \oplus G(x_0, x_1, x_2) \oplus$ $\oplus R_7(x_2 \oplus R_2(x_1 \oplus R_1(x_0)) \oplus R_6(x_1 \oplus R_1(x_0) \oplus R_5(x_0 \oplus R_4(x_3 \oplus G(x_0, x_1, x_2)))))$, де функція $G(x_0, x_1, x_2) = R_3(x_2 \oplus R_2(x_1 \oplus R_1(x_0)))$.

Візьмемо в якості функції $f(x, b) = \left[E_k(x, \alpha^{(0)}, \alpha^{(1)}, \beta_b)\right]_{y_1}$. Тоді ця функція має лінійну структуру $a = (G(\gamma_0) \oplus G(\gamma_1))\|1$.

Перевіримо цей факт.

$$f(x,b) \oplus f(x \oplus G(\gamma_0) \oplus G(\gamma_1), b \oplus 1) =$$
$$= x \oplus G(\gamma_b) \oplus R_7(\beta_b \oplus R_2(\alpha^{(1)} \oplus R_1(\alpha^{(0)})) \oplus$$
$$\oplus R_6(\alpha^{(1)} \oplus R_1(\alpha^{(0)}) \oplus R_5(\alpha^{(0)} \oplus R_4(x \oplus G(\gamma_b))))) \oplus x \oplus G(\gamma_0) \oplus G(\gamma_1) \oplus$$
$$\oplus R_3(\beta_{b\oplus 1} \oplus R_2(\alpha^{(1)} \oplus R_1(\alpha^{(0)}))) \oplus R_7(\beta_{b\oplus 1} \oplus R_2(\alpha^{(1)} \oplus R_1(\alpha^{(0)})) \oplus$$
$$\oplus R_6(\alpha^{(1)} \oplus R_1(\alpha^{(0)}) \oplus R_5(\alpha^{(0)} \oplus R_4(x \oplus G(\gamma_0) \oplus G(\gamma_1) \oplus$$

$$\oplus R_3(\beta_{b\oplus 1} \oplus R_2(\alpha^{(1)} \oplus R_1(\alpha^{(0)})))))) = G(\gamma_b) \oplus G(\gamma_{b\oplus 1}) \oplus G(\gamma_0) \oplus G(\gamma_1) \oplus$$
$$\oplus R_7(\beta_b \oplus R_2(\alpha^{(1)} \oplus R_1(\alpha^{(0)})) \oplus R_7(\beta_{b\oplus 1} \oplus R_2(\alpha^{(1)} \oplus R_1(\alpha^{(0)})) =$$
$$R_7(\beta_0 \oplus R_2(\alpha^{(1)} \oplus R_1(\alpha^{(0)})) \oplus R_7(\beta_1 \oplus R_2(\alpha^{(1)} \oplus R_1(\alpha^{(0)})) = \kappa \equiv const$$

Отже, функція $f(x, b)$ має лінійну структуру $a = (G(\gamma_0) \oplus G(\gamma_1))\|1$, яку супротивник може ефективно відновити за допомогою квантового алгоритму Бернштейна-Вазірані.

□

Як бачимо, нам вдалося збільшити на три кількість раундів, які супротивник в змозі розпізнати. Це досягнуто за допомогою фіксації перших констант та використання квантового алгоритму Бернштейна-Вазірані замість квантового алгоритму Саймона. Дана атака простим чином узагальнюється на довільну кількість блоків d, що демонструє наступне твердження.

Твердження 2.13. *$(3d-2)$-раундова узагальнена мережа Фейстеля типу 1 вразлива до квантових атак розпізнавання на основі обраного відкритого тексту.*

Оскільки було замінено квантовий алгоритм Саймона на квантовий алгоритм Бернштейна-Вазірані, доцільно провести аналіз складності цієї атаки, та порівняти його з попередньою атакою.

Твердження 2.14. *Атака на $(3d-2)$-раундову узагальнену мережу Фейстеля типу 1 має складність $O((\frac{n}{d})^2)$ та потребує $(\frac{n}{d}+2)$ кубітів відповідно, де n – довжина блоку шифрування криптопримітиву в бітах, d – кількість блоків.*

Доведення.

Через те, що атака зводиться до використання квантового алгоритму Бернштейна-Вазірані, то весь аналіз представлений в роботі [13] застосовний і до цієї атаки, що доводить це твердження. □

Наслідок 2.8. *Десять раундів шифру CAST-256 не є стійкою псевдовипадковою підстановкою в квантовій моделі обчислень. Складність*

атаки на цю систему складе $1024 \cdot c$ *запитів до квантового оракула та потребує* 34 *кубіти пам'яті, де константа* $c \geq 1$.

2.5 Атака розпізнавання на узагальнену мережу Фейстеля типу 2 та 3

В даному розділі представлена атака на узагальнені мережі Фейстеля типу 2 та 3. Причиною того, що атака застосовується відразу до двох типів є те, що в ході дослідження узагальнених мереж Фейстеля, для другого типу не було знайдено більш ефективних атак ніж атака загального виду для мережі типу 3. Оскільки мережа типу 2 є частковим випадком мережі типу 3, то ця атака також застосовна і до цього типу.

Причиною того, що для мережі типу 2 не було знайдено більш ефективних атак є те, що техніка для побудови атак використана раніше, опиралась на той факт, що існувала певна більша одиниці кількість раундів, для якої певні блоки шифрування залишаються незмінним, і лише зміщувались. Для мережі типу 2 це число раундів дорівнює одиниці, що унеможливлює використання атак такого типу.

Розглянемо атаку на прикладі узагальненої мережі Фейстеля типу 3. Ця атака, як було сказано раніше залишається коректною і для мережі типу 2 також. Тоді маємо наступне твердження.

Твердження 2.15. *Чотирираундова узагальнена мережа Фейстеля типу 3 вразлива до квантових атак розпізнавання на основі обраного відкритого тексту.*

Доведення.

Побудуємо атаку на чотири раунди узагальненої мережі Фейстеля типу 3.

Для атаки розглянемо третій блок шифротексту y_3. Він має вигляд $x_3 \oplus R_1(x_2) \oplus R_2(x_2 \oplus R_1(x_1)) \oplus R_3(x_2 \oplus R_1(x_1) \oplus R_2(x_1 \oplus R_1(x_0)))$.

Введемо нові позначення. Нехай $G(x_0, x_1, x_2) = R_1(x_2) \oplus R_2(x_2 \oplus R_1(x_1)) \oplus R_3(x_2 \oplus R_1(x_1) \oplus R_2(x_1 \oplus R_1(x_0)))$.

Нехай $\gamma_0 = (\alpha^{(0)}, \alpha^{(1)}, \beta_0)$ та $\gamma_1 = (\alpha^{(0)}, \alpha^{(1)}, \beta_1)$, $\beta_0 \neq \beta_1$ – фіксовані повідомлення. Тобто визначимо вектори в яких перші два блоки є однаковими, а останні – відрізняються. $E_k(x_0, x_1, x_2, x_3) = (y_0, y_1, y_2, y_3)$ – повне шифруюче перетворення.

Візьмемо в якості функції $f(x, b) = \left[E_k(\alpha^{(0)}, \alpha^{(1)}, \beta_b, x)\right]_{y_3}$. Тоді ця функція має період $s = (G(\gamma_0) \oplus G(\gamma_1))\|1$.

Перевіримо цей факт простою підстановкою.

$$f(x \oplus G(\gamma_0) \oplus G(\gamma_1), b \oplus 1) = \left[E_k(\alpha^{(0)}, \alpha^{(1)}, \beta_{b\oplus 1}, x \oplus G(\gamma_0) \oplus G(\gamma_1))\right]_{y_3} =$$
$$= x \oplus G(\gamma_0) \oplus G(\gamma_1) \oplus G(\gamma_{b\oplus 1}) = x \oplus G(\gamma_0) \oplus G(\gamma_1) \oplus \delta_{b,1} G(\gamma_0) \oplus \delta_{b,0} G(\gamma_1) =$$
$$= x \oplus G(\gamma_b) = f(x, b).$$

Отже, функція має деякий період s, який супротивник ефективно відновлює за допомогою квантового алгоритму Саймона. □

Наслідок 2.9. *Чотири раунди шифру RC6 не є стійкою псевдовипадковою підстановкою в квантовій моделі обчислень.*

Наступним кроком є узагальнення цього результату на довільну кількість підблоків d. В наслідок того, що для узагальненої мережі Фейстеля типу 3 вже для d раундів аналітичне представлення блоків шифротексту є достатньо складним, тому ми не маємо можливості провести пряме доведення, як було зроблено до цього. Проте якщо показати, що останній блок шифротексту має вигляд $x_{d-1} \oplus G(x_0, \ldots, x_{d-2})$, де структура функції функція $G(\cdot)$ складним чином залежить від кількості блоків d. Цей факт доведено в наступному твердженні.

Твердження 2.16. *Нехай $y_i^{(j)}$ – i-ий блок шифротексту j-го раунду узагальненої мережі Фейстеля типу 3. Тоді $\forall k = \overline{1, (d-1)} : y_{d-1-k}^{(k)} = x_{d-1} \oplus G_k(x_0, \ldots, x_{d-2})$, де $G_k(\cdot)$ – деяка функція, структура якої залежить від поточного раунду та їх загальної кількості.*

Доведення.

Доведення цього твердження прямим чином слідує з структури раундового перетворення узагальненої мережі Фейстеля типу 3. Воно має вигляд $F_i(x_0, \ldots, x_{d-1}) = (x_1 \oplus R_i(x_0), x_2 \oplus R_i(x_1), \ldots, x_{d-1} \oplus R_i(x_{d-2}), x_0)$, де

$R_i(x)$ – деяке невідоме перетворення на секретному ключі.

Доведемо це твердження методом індукції.

Нехай $k = 1$ – база індукції. Тоді шифротекст $y^{(1)}_{d-2} = F_1(x_0, \ldots, x_{d-1}) =$
$= \Big[(x_1 \oplus R_1(x_0), x_2 \oplus R_1(x_1), \ldots, x_{d-1} \oplus R_1(x_{d-2}), x_0)\Big]_{y^{(1)}_{d-2}} = x_{d-1} \oplus R_1(x_{d-2})$.
Візьмемо в якості $G(x_0, \ldots, x_{d-2}) = R_1(x_{d-2})$, тоді доводимо базу індукції.

Припустимо, що для деякого $k < d - 1$ виконується $y^{(k)}_{d-1-k} = x_{d-1} \oplus G_k(x_0, \ldots, x_{d-2})$. Тоді розглянемо наступний крок індукції.

Розглянемо блок шифротексту $y^{(k+1)}_{d-2-k} = F_{k+1}(y^{(k)}_0, \ldots, y^{(k)}_{d-1}) =$
$= \Big[(y^{(k)}_1 \oplus R_{k+1}(y^{(k)}_0), y^{(k)}_2 \oplus R_{k+1}(y^{(k)}_1), \ldots, y^{(k)}_{d-1} \oplus R_{k+1}(y^{(k)}_{d-2}), y^{(k)}_0)\Big]_{y^{(k+1)}_{d-2-k}} =$
$= y^{(k)}_{d-1-k} \oplus R_{k+1}(y^{(k)}_{d-2-k})$.

У випадку коли $k < d - 1$, блок шифротексту $y^{(k)}_{d-2-k}$ є функцією від змінних $x_0, \ldots, x_{d-2}$, серед яких можуть бути несуттєві змінні.

Тоді $y^{(k+1)}_{d-2-k} = y^{(k)}_{d-1-k} \oplus R_{k+1}(y^{(k)}_{d-2-k}) = x_{d-1} \oplus G_{d-1-k}(x_0, \ldots, x_{d-2}) \oplus$
$\oplus R_{k+1}(P(x_0, \ldots, x_{d-2})) = x_{d-1} \oplus G_{d-2-k}(x_0, \ldots, x_{d-2})$, що й потрібно було довести.

Отже, $\forall k = \overline{1, (d-1)} : y^{(k)}_{d-1-k} = x_{d-1} \oplus G_k(x_0, \ldots, x_{d-2})$.

□

Зауваження. З вигляду функції $y^{(k)}_{d-1-k} = x_{d-1} \oplus G_k(x_0, \ldots, x_{d-2})$ випливає, що можна варіювати індексом b будь яка змінну $x_0, \ldots, x_{d-2}$ або довільну їх комбінацію.

Маючи це твердження можемо сформулювати твердження про стійкість узагальненої мережі Фейстеля типу 3 до квантових атак розпізнавання.

Твердження 2.17. *d-раундова узагальнена мережа Фейстеля типу 3 вразлива до квантових атак розпізнавання на основі обраного відкритого тексту.*

Доведення. Відповідно до твердження доведеного вище для d-раундової узагальненої мережі Фейстеля типу 3 з d блоками, на $d-1$ раунді $y_0^{(d-1)} = x_{d-1} \oplus G(x_0, \ldots, x_{d-2})$, де $G(\cdot)$ – деяка функція структура якої залежить від кількості блоків d.

Оскільки при раунді шифрування перший блок без змін переміщається на останню позицію, то на раунді d блок шифрування $y_{d-1}^{(d)} = y_0^{(d-1)} = x_{d-1} \oplus G(x_0, \ldots, x_{d-2})$.

Тоді виберемо деяке число $k < d$ – кількість констант, які будемо варіювати. Нехай $\{\alpha^{(i)}\}_{i=0}^{d-2-k}$ – множина деяких фіксованих повідомлень, $\{\beta_0^{(i)}, \beta_1^{(i)}\}_{i=0}^{k}$ – множина парних констант, таких що $\beta_0^{(i)} \neq \beta_1^{(i)}$. Визначимо також $\sigma(x_0, \ldots, x_{d-2})$ – деяка перестановка. Нехай вектори $\gamma_b = \sigma(\alpha^{(0)}, \ldots, \alpha^{(d-2-k)}, \beta_b^{(0)}, \ldots, \beta_b^{(k)})$.

Визначимо функцію $f(x,b) = \left[E_k(\gamma_b, x)\right]_{y_{d-1}} = x \oplus G(\gamma_b)$. Тоді ця функція має період $s = (G(\gamma_0) \oplus G(\gamma_1))\|1$.

Дійсно, $f(x \oplus G(\gamma_0) \oplus G(\gamma_1), b \oplus 1) =$

$= \left[E_k(\gamma_{b\oplus 1}, x \oplus G(\gamma_0) \oplus G(\gamma_1))\right]_{y_{d-1}} = x \oplus G(\gamma_0) \oplus G(\gamma_1) \oplus G(\gamma_{b\oplus 1}) =$

$= x \oplus G(\gamma_0) \oplus G(\gamma_1) \oplus \delta_{b,1} G(\gamma_0) \oplus \delta_{b,0} G(\gamma_1) = x \oplus G(\gamma_b) = f(x,b).$

Отже, до цієї функції можна застосувати квантовий алгоритм Саймона, який ефективно знаходить значення $s = (G(\gamma_0) \oplus G(\gamma_1))\|1$, що й буде атакою на криптопримітив. □

Часова складність цієї атаки дорівнює $O(\frac{n}{d})$ та потребує $\frac{2n}{d}$ кубітів, як пряме використання квантового алгоритму Саймона, де n – довжина блоку шифрування криптопримітиву в цілому в бітах.

2.6 Атака розпізнавання на незбалансовану мережу Фейстеля

Далі будемо розглядати незбалансовану мережу Фейстеля в якій довжина правого блоку ділиться на довжину лівого блоку. Тоді структуру раундового перетворення можна замінити на еквівалентну структуру

$F_k(x_l, x_r) = F_k(x_0, \ldots, x_{d-1}) = (x_1, \ldots, x_{d-1}, x_0 \oplus R_k(x_1, \ldots, x_{d-1})$ (рис. 2.1), де кількість блоків $d = \frac{|x_r|}{|x_l|} + 1$.

Структура цієї мережі дуже схожа на узагальнену мережу Фейстеля типу 3, проте оскільки нелінійне перетворення застосовується до групи блоків, а не до кожного окремо, то це в загальному випадку додає певної стійкості в класичній моделі обчислень. Для квантових атак з використанням алгоритму Саймона така зміна структури є суттєвою і зазвичай значно погіршує атаку, проте для цього випадку погіршення атаки не відбудеться, хоча й в загальному ця атака буде достатньо слабкою, так як і атака на узагальнену мережу Фейстеля типу 3.

Оскільки атака є достатньо простою, відразу сформулюємо загальний випадок для d блокової мережі.

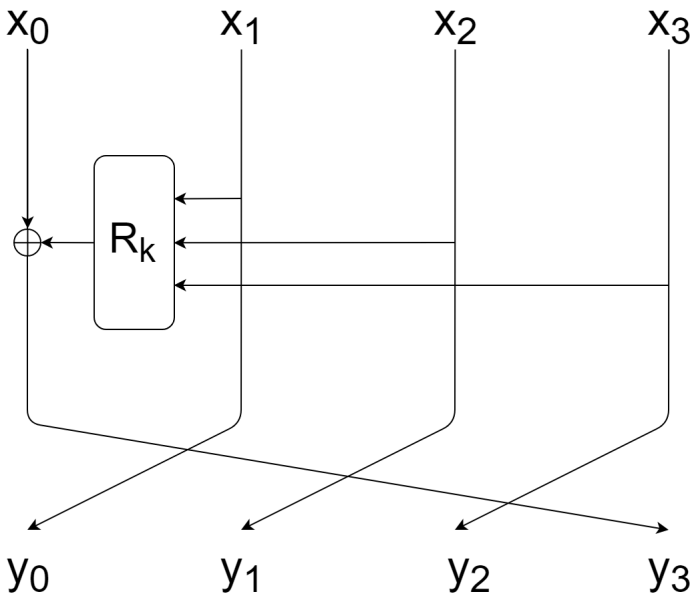

Рисунок 2.1 – Незбалансована мережа Фейстеля з кратними довжинами блоків

Твердження 2.18. *d-раундова незбалансована мережа Фейстеля вразлива до квантових атак розпізнавання на основі обраного відкритого тексту.*

Доведення. Побудуємо атаку на цю криптосистему. Розглянемо

перший блок шифротексту після d раундів шифрування.

Після першого раунду шифрування перший блок шифротексту дорівнює $y_0^{(1)} = x_0 \oplus R_1(x_1, \ldots, x_{d-1})$. Після другого раунду шифрування цей же блок шифротексту буде мати значення $y_0^{(2)} = x_1 \oplus R_2(x_2, \ldots, x_{d-1}, x_0 \oplus R_1(x_1, \ldots, x_{d-1}))$. Наступні $d-2$ раундів значення цього блоку не буде змінюватись, а лише зсуватись. Тоді матимемо наступну рівність $y_1^{(d)} = y_0^{(2)}$.

Нехай β_0, β_1 – деякі не однакові фіксовані повідомлення. $\alpha_0, \ldots, \alpha_{d-3}$ – деякий довільний набір фіксованих повідомлень. $E_k(x_0, \ldots, x_{d-1})$ – повне шифруюче перетворення.

Визначимо функцію $f(x, b) = \beta_b \oplus \Big[E_k(x, \beta_b, \alpha_0, \ldots, \alpha_{d-3})\Big]_{y_1} =$
$= \beta_b \oplus y_1 = \beta_b \oplus \beta_b \oplus R_2(\alpha_0, \ldots, \alpha_{d-3}, x \oplus R_1(\beta_b, \alpha_0, \ldots, \alpha_{d-3})) =$
$= R_2(\alpha_0, \ldots, \alpha_{d-3}, x \oplus R_1(\beta_b, \alpha_0, \ldots, \alpha_{d-3}))$.

Тоді задана функція $f(x, b)$ має деякий період s, який дорівнює $(R_1(\beta_0, \alpha_0, \ldots, \alpha_{d-3}) \oplus R_1(\beta_1, \alpha_0, \ldots, \alpha_{d-3}))\|1$.

Дійсно, $f(x \oplus (R_1(\beta_0, \alpha_0, \ldots, \alpha_{d-3}) \oplus R_1(\beta_1, \alpha_0, \ldots, \alpha_{d-3}), b \oplus 1) =$
$= R_2(\alpha_0, \ldots, \alpha_{d-3}, x \oplus R_1(\beta_0, \alpha_0, \ldots, \alpha_{d-3}) \oplus R_1(\beta_1, \alpha_0, \ldots, \alpha_{d-3}) \oplus$
$\oplus R_1(\beta_{b\oplus 1}, \alpha_0, \ldots, \alpha_{d-3})) = R_2(\alpha_0, \ldots, \alpha_{d-3}, x \oplus R_1(\beta_b, \alpha_0, \ldots, \alpha_{d-3})) = f(x, b)$.

Отже, визначена функція f має період $s = (R_1(\beta_0, \alpha_0, \ldots, \alpha_{d-3}) \oplus R_1(\beta_1, \alpha_0, \ldots, \alpha_{d-3}))\|1$, який ефективно знаходиться за допомогою квантового алгоритму Саймона. □

Твердження 2.19. *Атака на d-раундову незбалансовану мережу Фейстеля, де d – кількість блоків, має часову складність $O(\frac{n}{d})$ та потребує $\frac{2n}{d}$ кубітів пам'яті.*

Доведення. Доведення цього твердження напряму випливає з аналізу складності алгоритму Саймона, через те, що атака зводиться до прямого використання квантового алгоритму Саймона до функції $f(x, b)$. □

2.7 Атака розпізнавання на структуру DES-X

Схема $DES\text{-}X$ була запропонована в якості підсилення існуючого блокового шифру DES. Причиною цього є те, що реалізація цієї схеми може бути побудована з використанням апаратної реалізації шифру DES, яких було достатньо багато в 1990-ті.

Шифр $DES\text{-}X$ описується дуже простим співвідношенням $DES\text{-}X_{k,k_1,k_2}(x) = k_2 \oplus DES_k(x \oplus k_1)$ (рис. 2.2). $DES\text{-}X$ є частковим випадком схеми Івена-Мансура, де в якості $S(x)$ було взято шифр DES на деякому секретному ключі. В даному випадку атака представлена в роботі [3] не є застосовною, оскільки супротивник немає змоги обчислити DES_k для деякого секретного ключа. Проте до даного шифру застосовні всі вище наведені атаки на основі алгоритму Саймона, як для узагальненої мережі Фейстеля першого типу.

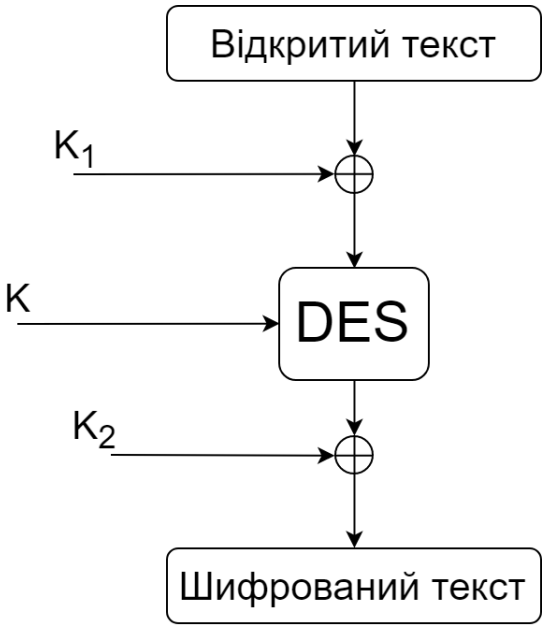

Рисунок 2.2 – Блоковий шифр DES-X

Твердження 2.20. *Трираундовий шифр $DES\text{-}X$ вразливий до квантових атак розпізнавання на основі обраного тексту.*

Доведення. $\alpha_1, \alpha_2 \in Z_2^{n/2}$ – фіксовані різні повідомлення, n –

довжина блоку шифрування в бітах, $(y_R, y_L) = DES_k(\alpha_b, x)$ – шифруюче перетворення, індекс $b \in \{0, 1\}$.

Визначимо функцію $f(x, b) = y_R \oplus \alpha_b = R_2(x \oplus R_1(\alpha_b))$, де $b \in \{0, 1\}$. Періодом цієї функції є значення $s = R_1(\alpha_0) \oplus R_1(\alpha_1)\|1$, отже, можна застосувати квантовий алгоритм Саймона для знаходження періоду цієї функції, що і буде безпосередньо атакою на таку мережу Фейстеля.

Визначимо аналогічну функцію $g(x, b) = y_R^{'} \oplus \alpha_b = f(x \oplus k_1) \oplus k_2$ для $(y_R^{'}, y_L^{'}) = DES\text{-}X_{k,k_1,k_2}(\alpha_b, x)$. Остільки k_2 деякий невідомий константний зсув, який однаковий при всіх шифруваннях, тому його можна відкинути та розглядати лише $f(x \oplus k_1)$. Тоді відповідно до узагальнення задачі Саймона визначеного вище, оскільки функції $g(x)$ та $f(x)$ пов'язані лише бієктивним перетворенням аргументу, то всі атаки, що були побудовані на DES, як мережу Фейстеля, залишаються коректними і для DES-X, з тією відмінністю, що константи α_b будуть зміщені на вектор k_1. □

Твердження 2.21. *Підсилення узагальненої мережі Фейстеля схемою Івена-Мансура залишає коректними усі вище зазначені атаки на основі алгоритму Саймона зі збереженням кількості раундів.*

Висновки до розділу 2

В розділі розглянуто отримані точні оцінки для складності алгоритму Саймона, які збігаються з асимптотичними оцінками відомими раніше. Узагальнено формулювання задачі Саймона та використаного його до криптоаналізу криптопримітиву на основі мережі Фейстеля. Побудовано атаки на узагальнені мережі Фейстеля типів 1, 2, 3 та незбалансовану мережу Фейстеля, методами диференціального квантового криптоаналізу з використанням алгоритмів Саймона та Бернштейна-Вазірані, застосовано отримані оцінки складності для алгоритму Саймона в аналізі складності цих атак.

ВИСНОВКИ

В результаті виконання роботи доведено можливість використання квантових алгоритмів Саймона та Бернштейна-Вазірані для криптоаналізу узагальнених мереж Фейстеля. Отримано точні оцінки для часової складності роботи алгоритму Саймона. Доведено, що цей алгоритм має лінійну часову та лінійну просторову складністі, та обчислено оцінки для математичного очікування та дисперсії кількості запитів до оракула, необхідних для алгоритму. Як наслідок, також підтверджено, що ймовірність того, що алгоритм ні коли не завершить роботу є нульовою на асимптотиці.

Узагальнено формулювання задачі Саймона на випадок функцій пов'язаних бієктивним перетворенням аргументу та використано це узагальнення для криптоаналізу схеми DES-X та їй подібних. На прикладі блокового шифру DES-X показано, що підсилення узагальнених схем Фейстеля схемою Івена-Мансура не підвищує стійкість узагальнених мереж Фейстеля до квантового диференціального криптоаналізу. Також отримано узагальнення формулювання задачі Саймона на випадок функцій, що мають неповні колізії. Доведено, що алгоритм Саймона коректно розв'язує й ці задачі, хоча у випадку функцій з неповними колізіями є необхідність модифікації алгоритму для додаткового розв'язку системи лінійних рівнянь зі спотвореною правою частиною. Наведено евристики для побудови фільтру системи векторів для розширеної задачі та запропоновано алгоритм фільтрації, що використовує ці евристики.

Досліджено стійкість узагальнених мереж Фейстеля до квантових атак на основі алгоритмів Саймона та Бернштейна-Вазірані. Як результат, суттєво покращено атаку на узагальнену мережу Фейстеля типу 1, у порівнянні з класичним узагальненням. Кількість раундів, для яких побудована квантова атака розпізнавання може мати значення $3d - 2$ включно, де d – це кількість блоків, при цьому маючи можливість робити

запити тільки до шифруючого оракула. Складність цієї часова атаки є поліноміальною і дорівнює $O((\frac{n}{d})^2)$ та використовує $\frac{n}{d} + 2$ кубітів пам'яті, де n – довжина блоку шифрування криптопримітиву вцілому. Ця складність є гіршою у порівнянні з алгоритмом Саймона, проте все одно експоненційно краща ніж будь-який класичний алгоритм розв'язку цієї задачі.

Для узагальнених мереж Фейстеля типу 2 не знайдено кращих атак, ніж атаки загального типу на узагальнену мережу Фейстеля типу 3, в наслідок конструктивних особливостей схеми типу 2. Для узагальнених мереж Фейстеля типу 3 знайдено загальну атаку розпізнавання, яка застосовна до узагальнених мереж Фейстеля всіх типів, проте ця атака є значно слабша ніж, атака на мережу типу 1. Вона дозволяє розпізнати d раундів узагальненої мережі Фейстеля, при часовій складності атаки $O(\frac{n}{d})$ та необхідності $\frac{2n}{d} + 1$ кубітів пам'яті, де n – довжина блоку шифрування криптопримітиву вцілому. Як приклад схожої конструкції досліджено незбалансовану мережу Фейстеля, та доведено, що для d-блокової незбалансованої мережі маємо атаку на ту ж кількість раундів, що й для узагальненої мережі Фейстеля типу 3, тобто d раундів шифрування. Ця атака має таку ж саму часову та просторову складність, що й атака на узагальнену мережу Фейстеля типу 3.

БІБЛІОҐРАФІЯ

[1] Kuwakado Hidenori, Morii Masakatu. Quantum Distinguisher Between the 3-Round Feistel Cipher and the Random Permutation. — 2010. — 06. — P. 2682–2685.

[2] Bonnetain Xavier, Naya-Plasencia Maria. Hidden Shift Quantum Cryptanalysis and Implications. — 2018. — 01. — P. 560–592. — ISBN: 978-3-030-03325-5.

[3] Breaking Symmetric Cryptosystems using Quantum Period Finding / Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, María Naya-Plasencia. — 2016. — 02.

[4] Santoli Thomas, Schaffner Christian. Using Simon's Algorithm to Attack Symmetric-Key Cryptographic Primitives. — 2016. — 03. — Vol. 17.

[5] Xie Huiqin, Yang Li. Using Bernstein–Vazirani algorithm to attack block ciphers // Designs, Codes and Cryptography. — 2019. — 05. — Vol. 87, no. 5. — P. 1161–1182. — Access mode: https://doi.org/10.1007/s10623-018-0510-5.

[6] Ito Gembu, Iwata Tetsu. Quantum Distinguishing Attacks against Type-1 Generalized Feistel Ciphers // IACR Cryptology ePrint Archive. — 2019. — Vol. 2019. — P. 327.

[7] Dong Xiaoyang, Li Zheng, Wang Xiaoyun. Quantum cryptanalysis on some generalized Feistel schemes // Science China Information Sciences. — 2019. — Jan. — Vol. 62, no. 2. — P. 22501. — Access mode: https://doi.org/10.1007/s11432-017-9436-7.

[8] Quantum Differential and Linear Cryptanalysis / Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, María Naya-Plasencia // IACR Transactions on Symmetric Cryptology. — 2015. — 10.

[9] Nielsen Michael A., Chuang Isaac L. Quantum Computation and Quantum Information. — Cambridge University Press, 2000.

[10] Rieffel Eleanor, Polak Wolfgang. Quantum Computing: A Gentle Introduction. — 1st edition. — The MIT Press, 2011. — ISBN: 9780262015066.

[11] Simon D. R. On the Power of Quantum Computation. — 1994. — P. 116–123. — Access mode: https://doi.org/10.1109/SFCS.1994.365701.

[12] Bernstein Ethan, Vazirani Umesh. Quantum Complexity Theory // SIAM J. Comput. — 1997. — Oct. — Vol. 26, no. 5. — P. 1411–1473. — Access mode: http://dx.doi.org/10.1137/S0097539796300921.

[13] Xie Huiqin, Yang Li. A quantum related-key attack based on Bernstein-Vazirani algorithm. — 2018. — 08.

[14] Luby Michael, Rackoff Charles. How to Construct Pseudorandom Permutations from Pseudorandom Functions // SIAM J. Comput. — 1988. — 04. — Vol. 17. — P. 373–386.

[15] Biryukov Alex, Wagner David. Slide Attacks // Fast Software Encryption / Ed. by Lars Knudsen. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1999. — P. 245–259.

[16] Zheng Yuliang, Matsumoto Tsutomu, Imai Hideki. On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. — 1989. — 01. — P. 461–480.

[17] Hoang Viet Tung, Rogaway Phillip. On Generalized Feistel Networks // Proceedings of the 30th Annual Conference on Advances in Cryptology. — CRYPTO'10. — Berlin, Heidelberg : Springer-Verlag, 2010. — P. 613–630. — Access mode: http://dl.acm.org/citation.cfm?id=1881412.1881455.